**Telma Daniela Pereira de Pinho**

# Realizações Mínimas de Espaço de Estados de Códigos Convolucionais 2D

# Minimal State-Space Realizations of 2D Convolutional Codes

**Telma Daniela Pereira de Pinho**

# Realizações Mínimas de Espaço de Estados de Códigos Convolucionais 2D

# Minimal State-Space Realizations of 2D Convolutional Codes

Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à obtenção do grau de Doutor em Matemática, realizada sob a orientação científica das Professoras Doutoras Maria Paula Macedo Malonek, Professora Catedrática do Departamento de Engenharia Electrotécnica da Faculdade de Engenharia da Universidade do Porto e Maria Raquel Rocha Pinto, Professora Auxiliar do Departamento de Matemática da Universidade de Aveiro

Apoio financeiro da FCT e do FSE no âmbito do III Quadro Comunitário de Apoio.

Para a minha irmã

**o júri**

presidente

**Doutor Vitor José Babau Torres**

Professor Catedrático da Universidade de Aveiro

**Doutor Joan Josep Climent Coloma**

Professor Catedrático da Universidade de Alicante–Espanha

**Doutor Ettore Fornasini**

Professor Catedrático da Universidade de Pádua-Itália

**Doutora Teresa Paula Coelho Azevedo Perdicoúlis**

Professora Auxiliar com Agregação da Universidade de Trás-Os-Montes e Alto Douro

**Doutora Maria Raquel Rocha Pinto**

Professora Auxiliar da Universidade de Aveiro (coorientadora)

**Doutor Diego Napp Avelli**

Investigador Auxiliar da Universidade de Aveiro

**agradecimentos**

Às professoras Paula Rocha e Raquel Pinto que desde o primeiro instante me encorajaram e inspiraram na minha descoberta da Teoria de Sistemas e da Teoria de Códigos. Por todo o apoio científico prestado ao longo destes anos, pela incansável paciência e disponibilidade, pelo carinho, o meu mais sincero obrigada.

Al professor Ettore Fornasini, per le innumerevoli ore passate con me condividendo la sua esperienza e la sua saggezza e dandomi preziosi suggerimenti per la mia ricerca attuale e futura. Grazie per avermi accolto in Italia e per avermi fatto sentire a casa.

À Universidade de Aveiro e em particular ao Departamento de Matemática, pelas condições de trabalho proporcionadas ao longo destes quatro anos. Ao Paolo Vettori por todo o apoio que me deu na utilização do programa LaTeX.

À Fundação para a Ciência e Tecnologia pelo apoio financeiro prestado.

Às minhas companheiras e amigas Carla e Catarina, pelo incentivo constante nos momentos mais difíceis e pelo ambiente sempre agradável que partilhámos.

Às "minhas pessoas" por terem estado sempre por perto, por tirarem o melhor de mim e por me fazerem sempre sentir especial.

Aos meus pais e irmãos pea estrutura familiar sólida e feliz que sempre me souberam dar, pela incessante transmissão de confiança, sem vocês seria impossível chegar aqui. Por tudo, obrigada.

Ao Tiago que é a minha maior referência de coragem e força. Obrigada por ter crescido contigo, obrigada por teres ficado sempre comigo.

**palavras-chave** Códigos Convolucionais 2D, Realizacões Mínimas, Modelos de Roesser Separáveis

**resumo** Nesta tese consideramos códigos convolucionais a duas dimensões (2D). Como acontece no caso unidimensional (1D) uma das questões fundamentais neste contexto diz respeito à obtenção de realizações mínimas de espaço de estados para estes códigos.

O problema da realizacão mínima de códigos não é equivalente ao problema da realizacão mínima de codificadores. Tal acontece uma vez que um dado código admite diferentes codificadores com diferentes graus de McMillan. Nesta tese, focamos a nossa atencão no estudo da minimalidade de realizações de códigos convolucionais 2D através de modelos de Roesser separáveis. Tais modelos podem ser encarados como a conexão em série de dois sistemas 1D.

Numa primeira fase propomos um procedimento que possibilita obter realizações mínimas de um código convolutional 1D a partir de realizações mínimas de um codificador desse código. De seguida, restringimos o nosso estudo a duas classes particulares de códigos convolucionais 2D. A primeira classe a ser considerada é a classe de códigos que admite codificadores do tipo $n \times 1$. Para estes códigos, são caracterizados os codificadores mínimos (i.e. codificadores para os quais uma realização mínima também é mínima enquanto realização do código), possibilitando a construção de realizações mínimas de códigos a partir dos seus codificadores mínimos. A segunda classe a ser considerada é a classe constituída por códigos a que demos o nome de "composition codes". Para uma subclasse destes códigos, propomos um método de obtenção de realizações mínimas através de modelos de Roesser separáveis.

**keywords** 2D Convolutional Codes, Minimal Realizations, Separable Roesser Models

**abstract** In this thesis we consider two-dimensional (2D) convolutional codes. As happens in the one-dimensional (1D) case one of the major issues is obtaining minimal state-space realizations for these codes.

It turns out that the problem of minimal realization of codes is not equivalent to the minimal realization of encoders. This is due to the fact that the same code may admit different encoders with different McMillan degrees. Here we focus on the study of minimality of the realizations of 2D convolutional codes by means of separable Roesser models. Such models can be regarded as a series connection between two 1D systems.

As a first step we provide an algorithm to obtain a minimal realization of a 1D convolutional code starting from a minimal realization of an encoder of the code. Then, we restrict our study to two particular classes of 2D convolutional codes. The first class to be considered is the one of codes which admit encoders of type $n \times 1$. For these codes, minimal encoders (i.e., encoders for which a minimal realization is also minimal as a code realization) are characterized enabling the construction of minimal code realizations starting from such encoders. The second class of codes to be considered is the one constituted by what we have called composition codes. For a subclass of these codes, we propose a method to obtain minimal realizations by means of separable Roesser models.

# Contents

# Introduction

Information is one of the most valuable assets nowadays, and efficient and reliable digital information transmission and data storage have become a major concern in the last decades.

The physical devices used to transmit and store information may be subject to noise, what can result in the loss of important data with respect to the original information. Error correcting codes are a key element to address this issue, which has been a subject of research in areas related to information. For instance, the recovery of a scratched CD or secure communication over power-limited devices in spacecrafts are possible due to the use of codes which enable the correction of errors and erasures that may occur in noisy transmission channels and physical devices.

In order to achieve a secure transmission process, sophisticated mathematical techniques have been implemented in such a way as to provide robust and time optimal coding and decoding schemes.

For every different code, there is an encoding map (or encoder) from the set of information messages to the set of all the codewords. This map adds to the information sufficient but finite redundancy to allow detecting and correcting the errors that might happen after channel transmission. An error is detected whenever the received message is not any of the codewords. The decoding process assigns to any received message a codeword having maximum probability of being the original sent one.

The origins of coding theory date back to the landmark work of Claude Shanon in his 1948 paper "A Mathematical Theory of Communication" [41]. The author showed that it is always possible to encode a message so that it can be sent with maximal reliability and minimal redundancy. In this way his main concerns were related to *data representation*

and *message transmission over a noisy channel*. However the proof was not constructive and codes with those capacities were not explicitly given. In turn, Hamming published in [16] the first well known code construction. But the properties of his codes revealed to be disappointing when compared with the stronger properties claimed by Shannon, and since then intensive research has been done in order to find better codes.

The first class of linear codes obtained were the block codes [24]. The conceptual leap to one dimensional (1D) convolutional codes was made by Peter Elias in 1955 [5], which has significantly improved the research in coding theory. Such codes became popular after the invention of attractive decoding algorithms such as sequential decoding by Wozencraft [47], threshold decoding by Massey [25], and the Viterbi algorithm [44], as referred in [13]. Enforcement of 1D convolutional codes has proven to be most advantageous in diverse situations, and triggered some connections between systems theory and 1D convolutional coding by describing a convolutional encoder as a transfer function of a linear, time-invariant system over a (finite) field [26, 27]. A general algebraic theory for 1D convolutional codes was first formalized by Forney [11] and then by Piret [32] and McEliece [28], greatly influenced by the foundation work of Kalman [19] with respect to realization theory through state-space models. In [11, 12] Forney showed that the algebraic theory of multivariable systems is the natural setting for the algebraic theory of 1D convolutional codes. It should be noted that Forney reformulated the work on 1D convolutional codes developed in [11] in the paper [12], targeted for the systems theory community. Since then these two papers [11, 12] constitute an essential tool in the context of multivariable linear system theory. A detailed review of the literature on this subject can be found in [31].

However, while the classical approach to systems theory focuses on input/output relations, the interest of coding theory concerns the set of output sequences produced by the encoder, since robustness of error correction and/or detection of errors introduced during transmission only depends on properties of the set of codewords, i.e., of the code. This difference leads to a new perspective on the subject.

The behavioral approach to dynamical systems, introduced by Willems [46] in the eighties, views a system essentially as a set constituted by all trajectories that are compatible

with the described phenomenon. Such admissible set of trajectories is known as the system behavior.

This innovative approach is close to the coding situation, as a convolutional code can be regarded as a linear, time-invariant behavior, whereas an encoder is a representation of this behavior (code).

Concerning the 1D case, Fornasini and Pinto, [9], considered the behavioral approach to systems theory to present a new definition of convolutional code over a finite field constituted by left compact sequences. In the analysis of the encoders of such codes, which are rational matrices, they used Matrix Fraction Descriptions (MFD's) and have characterized some properties of the encoders and the structure of the code. These authors also studied the problem of obtaining minimal state-space realizations of codes, via the minimal state-space realization of encoders with minimal McMillan degree, called minimal encoders.

Meanwhile a very active area of research concerns the higher dimensional (nontrivial) generalizations of one-dimensional (1D) convolutinal codes. In this thesis we focus on two-dimensional (2D) convolutional codes. These codes may prove to be useful in transmission and storage of 2D sequences of data such as images, pictures or video images. In order to encode data recorded in two directions it is currently usual to transform it into arrays of 1D sequences by means of scanning in one direction, and then apply 1D encoding techniques, ignoring the interdependence in the other direction. However, it is possible and desirable to work within a structure that takes advantages of the correlation of the data in the two directions. Such structure leads to 2D convolutional codes, generalizing the notion of 1D convolutional codes. Given the inherent differences between 1D and 2D cases, this generalization is nontrivial. Although 1D convolutional codes have been widely understood, the same does not happens for the 2D case. Fundamental issues related with the detection and correction of errors or decoding algorithms that are well known for the 1D case have not yet been exploited in the framework of 2D convolutional codes. Only recently, the first steps in the construction of robust 2D convolutional codes were done by Climent *et al.* [3]. Most of the existing research is focused on algebraic aspects and fundamental issues. The first attempts to develop the general theory and the basic algebraic properties of 2D convolutional

codes were proposed in [10] where Fornasini and Valcher introduced 2D convolutional codes constituted by sequences indexed by $\mathbb{Z}^2$, and discussed issues as the characterization of such codes in terms of their internal properties and input-output representations. Later, in [43], the same authors considered 2D convolutional codes in which the codewords admit compact support in $\mathbb{Z}^2$, and presented several properties of their encoders and syndrome formers (parity-check matrices) under different hypotheses on the code structure.

In [45], Weiner studied for the first time the multidimensional (nD) convolutional codes having finite support in $\mathbb{N}^n$. In [15], Gluesing-Luerssen, Rosenthal and Weiner analyzed the connections between (nD) convolutional codes and (nD) systems. More recently, for the purpose of studying (nD) convolutional codes from a more practical point of view, R. Lobo introduced in [22] the concept of *locally invertible encoders* and the *Tail-Biting convolutional codes* with the aim of obtaining constructions of 2D convolutional codes with particular decoding properties. Recently, Napp *et al.* [29] generalized to the 2D case the input-state-output representations of 1D convolutional codes defined by Rosenthal and collaborators [38, 40].

In this thesis we study 2D convolutional codes through mathematical techniques used in systems theory for the 2D case. Concretely, following the approach already used by several authors for the 1D case, we consider two-dimensional (2D) convolutional codes over a field $\mathbb{F}$, constituted by 2D bilateral sequences that are generated by a specific type of encoders, the polynomial ones. Both encoders and codes admit representations by means of 2D state-space models. Our main purpose is to study the code realization problem for the 2D case with special focus in obtaining realizations of minimal dimension. This is motivated not only by a reduction of the computational costs, but also by the importance of the use of minimal realizations in the search for convolutional codes with suitable properties, such as a good distance. The construction of convolutional codes with good distance, i.e., with good capability of error correction, is in general a hard problem. Minimal state-space realizations have been used to construct 1D convolutional codes of a given rate and a prescribed distance [37, 38, 40, 42]. Only recently, constructions of 2D convolutional codes with a designed distance were obtained [29, 30]. In [29] minimal realizations based on the Fornasini-Marchesini

model were used to construct such codes. However, the minimality of such models is not characterized, restricting its application in the search of new constructions.

Although one can choose among different state-space models for 2D processes [1, 7, 35], we have opted to consider here separable Roesser models, due to the simplicity of their updating scheme. Indeed, these models can be viewed as the series connection of two 1D state-space models each of which evolves in a different direction. This special structure allowed giving a characterization of minimality in terms of necessary and sufficient conditions on the system matrices (similar to the 1D case) [17], which is not possible to achieve for other types of models. Separable Roesser models do not realize all 2D-causal transfer-functions, but only those which have a separable denominator, i.e., whose denominator is the product of two 1D polynomials, each of which in a different variable. Fortunately, 2D polynomial encoders (to which we restrict in this thesis) can be regarded as separable denominator transfer functions, and hence admit a realization by means of separable Roesser models. In this framework, we first consider the realization of 2D convolutional codes by a similar procedure to the one used in [9] for the 1D case, i.e., by first finding a minimal 2D polynomial encoder and then obtaining a minimal separable Roesser realization of that encoder. It turns out that the characterization of minimal 2D encoders is a hard problem, that could not be solved with full generality. Nevertheless, we provide a characterization of minimal encoders for the particular class of 2D convolutional codes of rate $1/n$.

As for the case of codes of general rate $k/n$, we consider a particular class of 2D convolutional encoders and corresponding convolutional codes, that we respectively call composition encoders and composition codes, and show that, under certain conditions, composition encoders are minimal. Moreover, for the encoders that satisfy these minimality conditions, minimal 2D state-space realizations are obtained, yielding minimal realizations of the corresponding 2D convolutional codes.

Although there is still much to be done in this topic, we believe that minimal realizations via separable Roesser models constitute a good framework for the construction of optimal 2D convolutional codes.

We next give a brief outline of the contents of each chapter of this thesis.

**Chapter 1 - Preliminaries**

This chapter contains some definitions and results about polynomial matrices in one and two indeterminates. Particular classes of polynomial matrices will play a fundamental role in the analysis of both polynomial 1D and 2D encoders and therefore further properties as unimodularity and primeness are highlighted both for the 1D and the 2D cases.

**Chapter 2 - Convolutional codes and their encoders**

In this chapter we begin by introducing the notion of 1D convolutional codes, and some necessary background such as properties of equivalent encoders are presented. Some of the results on encoders that will be considered are well known, and are presented without proof, together with the reference to the papers or standard textbook(s) where a proof is provided. We opted to collect here these results for the sake of completeness. We introduce here a class of encoders similar to the well known *systematic* encoders, which we have called *quasi-systematic* encoders, as they are considered latter in this study. In a second stage a natural extension of 1D convolutional codes and their encoders is considered for the 2D case.

**Chapter 3 - The realization problem**

The realization problem is considered, focusing on the study of the minimal realization of 1D encoders and of the corresponding convolutional codes. Moreover this problem is investigated in the light of Willems's behavioral approach, and a procedure for obtaining a minimal realization of a 1D encoder which is also a minimal realization of the corresponding code is provided. Concerning the 2D case, Roesser state-space models are introduced, and special attention is given to the separable case. The final part of this chapter is devoted to an overview of the sufficient conditions for minimality of 2D convolutional codes derived from results already available in the literature.

**Chapter 4 - Minimal realization of 2D convolutional codes**

The minimality of 2D convolutional codes is characterized for a particular class of encoders, namely the ones of type $n \times 1$ (rate $1/n$), and some considerations on the generalization of the presented results for encoders of type $n \times k$ (i.e., rate $k/n$), for $k > 1$ are made to highlight the main achievements reached and the experienced difficulties.

**Chapter 5 - Composition codes**

A particular class of 2D convolutional codes (composition codes) whose encoders can be decomposed as the product of two 1D encoders, each one in one direction/indeterminate is introduced. We prove that under certain conditions, composition encoders are minimal. Moreover, for the encoders that satisfy the minimality conditions, minimal 2D state-space realizations are obtained, which are minimal realizations of the corresponding 2D convolutional codes.

**Chapter 6 - Conclusions**

Finally, in the last chapter, we summarize the main results and discuss some future work to be carried out.

# Chapter 1

# Preliminaries

Polynomial matrices constitute an essential tool in the study of problems such as modeling linear systems in the behavioral approach or concerning convolutional codes. Although we present here well known results, that could have been given in an appendix, we opted to collect them in this chapter due to their relevance for polynomial encoders to which we give particular attention throughout this thesis. After presenting some definitions and results in the 1D case, we consider the 2D case. For more details we refer to [6, 14, 18] for the 1D case and to [10, 23, 33, 43] for the 2D case.

## 1.1 1D polynomial matrices

Let us consider a field $\mathbb{F}$ and denote, as usually, by $\mathbb{F}[d]$ and $\mathbb{F}(d)$ the ring of polynomials in $d$ and the field of rational functions with coefficients in $\mathbb{F}$, respectively. Denote by $\mathbb{F}[d]^{n\times k}$ the set of matrices of size $n \times k$ with elements in $\mathbb{F}[d]$.

We start by considering a very important class of polynomial matrices known as *unimodular* matrices. Such matrices are those who admit a polynomial inverse as defined below.

**Definition 1.1.** A matrix $U(d) \in \mathbb{F}[d]^{k\times k}$ is *unimodular* if it is invertible in $\mathbb{F}[d]^{k\times k}$, i.e., if there exists $V(d) \in \mathbb{F}[d]^{k\times k}$ such that

$$V(d)U(d) = U(d)V(d) = I_k.$$

The next proposition characterizes the class of unimodular matrices.

**Proposition 1.2.** *Let $U(d) \in \mathbb{F}[d]^{k\times k}$. The following are equivalent:*

*(i)* $U(d)$ *is unimodular;*

*(ii)* $\det U(d) = \alpha, \quad$ *where* $\quad \alpha \in \mathbb{F} \setminus \{0\}$.

Unimodular matrices play the same role as the nonzero constants in polynomial factorization.

The concepts of divisor (or factor) of a polynomial and common divisor of a pair of polynomials can be extended to the matricial case. However, due to the non-commutativity of the product of matrices is necessary to distinguish between left and right factors. In the sequel, definitions and results are stated only for the "right" case as the "left" case is entirely analogous.

**Definition 1.3.** Let $G(d) \in \mathbb{F}[d]^{n\times k}$.

(i) $\Delta(d) \in \mathbb{F}[d]^{k\times k}$ is a *right-divisor* of $G(d)$ if

$$G(d) = \bar{G}(d)\Delta(d), \tag{1.1}$$

for some $\bar{G}(d) \in \mathbb{F}[d]^{n\times k}$.

(ii) $\Delta(d) \in \mathbb{F}[d]^{k\times k}$ is called a *right maximal divisor* (rMD) of $G(d)$ if (1.1) holds and

$$G(d) = \bar{G}(d)\tilde{\Delta}(d),$$

with $\tilde{\Delta}(d) \in \mathbb{F}[d]^{k\times k}$ and $\bar{G}(d) \in \mathbb{F}[d]^{n\times k}$, implies that there exist $F(d) \in \mathbb{F}[d]^{k\times k}$ such that $\Delta(d) = F(d)\tilde{\Delta}(d)$.

Matrices without nonunimodular factors (divisors) play an important role on matrix factorization and are called *right-prime* matrices. This class of matrices is defined and characterized below.

**Definition 1.4.** A polynomial matrix $G(d) \in \mathbb{F}[d]^{n\times k}$ is *right-prime* if in all factorizations

$$G(d) = \bar{G}(d)\Delta(d), \quad \Delta(d) \in \mathbb{F}[d]^{k\times k}, \quad \bar{G}(d) \in \mathbb{F}[d]^{n\times k},$$

the right-factor $\Delta(d)$ is unimodular.

Further properties of right-prime matrices are stated in the following lemma.

**Lemma 1.5.** *[18] Let $G(d) \in \mathbb{F}[d]^{n\times k}$.*

*(i)* $\Delta(d) \in \mathbb{F}[d]^{k\times k}$ *is a rMD of* $G(d)$ *if and only if* $G(d) = \bar{G}(d)\Delta(d)$*, for some right-prime matrix* $\bar{G}(d) \in \mathbb{F}[d]^{n\times k}$.

*(ii) If* $G(d) = \bar{G}(d)U(d)$*, with* $U(d) \in \mathbb{F}[d]^{k\times k}$ *unimodular and* $\bar{G}(d) \in \mathbb{F}[d]^{n\times k}$ *right-prime, then* $G(d)$ *is also right-prime.*

*(iii) If* $G(d)$ *is right-prime then it has full column rank.*

Note that, if $G(d) \in \mathbb{F}[d]^{n\times k}$ is a right-prime matrix, then $k \leq n$.

In general, it is not easy to check by the definition whether a matrix is right-prime or not. However, the next result (in particular condition (iv)) provides an easier way to check this property.

**Proposition 1.6.** *[6, 18] Let* $G(d) \in \mathbb{F}[d]^{n\times k}$*, with* $n \geq k$*. The following are equivalent:*

*(i)* $G(d)$ *is right-prime.*

*(ii) There exists* $H(d) \in \mathbb{F}[d]^{n\times(n-k)}$ *such that* $\begin{bmatrix} G(d) & H(d) \end{bmatrix}$ *is unimodular.*

*(iii)* $G(d)$ *admits a polynomial left inverse.*

*(iv) The greatest common divisor (GCD) of the* $k$*-th order minors of* $G(d)$ *is* 1.

*(v) For all* $\hat{u}(d) \in \mathbb{F}(d)^{k\times 1}$*,* $G(d)\hat{u}(d) \in \mathbb{F}[d]^{n\times 1}$ *implies* $\hat{u}(d) \in \mathbb{F}[d]^{n\times 1}$.

*(vi)* $G(\alpha)$ *has rank* $k$*, for all* $\alpha \in \bar{\mathbb{F}}$*, where* $\bar{\mathbb{F}}$ *denotes the algebraic closure of* $\mathbb{F}$.

The definitions and results related to the notion of factors of a polynomial matrix can be extended in a similar way when we are dealing with a pair of polynomial matrices.

**Definition 1.7.** Let $G_1(d) \in \mathbb{F}[d]^{n_1\times k}$ and $G_2(d) \in \mathbb{F}[d]^{n_2\times k}$. Then $\Delta(d) \in \mathbb{F}[d]^{k\times k}$ is a *right common divisor* of $G_1(d)$ and $G_2(d)$ if

$$G_1(d) = \bar{G}_1(d)\Delta(d) \quad \text{and} \quad G_2(d) = \bar{G}_2(d)\Delta(d), \tag{1.2}$$

for some $\bar{G}_1(d) \in \mathbb{F}[d]^{n_1\times k}$ and $\bar{G}_2(d) \in \mathbb{F}[d]^{n_2\times k}$.

Note that if $\Delta(d)$ is a right common divisor of $G_1(d)$ and $G_2(d)$ then (1.2) is equivalent to

$$\begin{bmatrix} G_1(d) \\ G_2(d) \end{bmatrix} = \begin{bmatrix} \bar{G}_1(d) \\ \bar{G}_2(d) \end{bmatrix} \Delta(d),$$

and consequently, $\Delta(d)$ is a right-factor of $\begin{bmatrix} G_1(d) \\ G_2(d) \end{bmatrix}$.

**Definition 1.8.** $G_1(d) \in \mathbb{F}[d]^{n_1 \times k}$ and $G_2(d) \in \mathbb{F}[d]^{n_2 \times k}$ are *right-coprime* if all their right common factors are unimodular.

The next corollary follows from Proposition 1.6.

**Corollary 1.9.** *[6] Let $G_1(d) \in \mathbb{F}[d]^{n_1 \times k}$ and $G_2(d) \in \mathbb{F}[d]^{n_2 \times k}$. The following are equivalent:*

1. *$G_1(d)$ and $G_2(d)$ are right-coprime.*
2. *The matrix $\begin{bmatrix} G_1(d) \\ G_2(d) \end{bmatrix}$ is right-prime.*
3. *There exist $X_1(d) \in \mathbb{F}[d]^{k \times n_1}$ and $X_2(d) \in \mathbb{F}[d]^{k \times n_2}$ such that the Bézout equation*

$$X_1(d)G_1(d) + X_2(d)G_2(d) = I_k,$$

*holds.*

Let us now introduce some definitions and results concerning the degree of a polynomial matrix.

The degree of a polynomial row or column is defined as the maximum degree of its entries. Taking this notion into account, let us state the following definition.

**Definition 1.10.** Let $G(d) \in \mathbb{F}[d]^{n \times k}$ with column degrees given by $\ell_1, \ldots, \ell_k$.

(i) The *external degree* of $G(d)$, $\operatorname{ext\,deg}(G(d))$, is the sum of its column degrees, i.e.,

$$\operatorname{ext\,deg}(G(d)) = \sum_{i=1}^{k} \ell_i.$$

(ii) The *internal degree* of $G(d)$, $\operatorname{int\,deg}(G(d))$, is the maximum degree of its $k$-th order minors.

Since the computation of the $k$-th order minors may lead to the cancelation of the monomials of highest degree, $\operatorname{int\,deg}(G(d)) \leq \operatorname{ext\,deg}(G(d))$, for any $G(d) \in \mathbb{F}[d]^{n\times k}$. The internal and external degrees of a polynomial matrix are associated with the notion of another class of matrices, the *column reduced* matrices, which we define below.

**Definition 1.11.** A polynomial matrix $G(d) \in \mathbb{F}[d]^{n\times k}$ with rank $k$ and column degrees $\ell_1, \ldots, \ell_k$ is *column reduced* if at least one of its minors of order $k$ has degree $\sum_{i=1}^{k} \ell_i$, i.e., if

$$\operatorname{int\,deg}(G(d)) = \operatorname{ext\,deg}(G(d)). \tag{1.3}$$

The next proposition concerns the reduction of polynomial matrices to column reduced form and will play an important role in the next chapter.

**Proposition 1.12.** *[18, 6]*

*(i) If $G_1(d), G_2(d) \in \mathbb{F}[d]^{n\times k}$ are column reduced and $G_1(d) = G_2(d)U(d)$, for $U(d) \in \mathbb{F}[d]^{k\times k}$ unimodular, then, up to a permutation, the column degrees of $G_1(d)$ and $G_2(d)$ are the same.*

*(ii) If $G(d) \in \mathbb{F}[d]^{n\times k}$, there exists a unimodular matrix $U(d) \in \mathbb{F}[d]^{k\times k}$ such that $G(d)U(d)$ is column reduced and, by (i), the column degrees of $G(d)U(d)$ are uniquely determined, up to a permutation.*

## 1.2 2D polynomial matrices

In this section similarly to what was done in the 1D case, some definitions and results concerning 2D polynomial matrices are presented.

Let us denote by $\mathbb{F}[d_1, d_2]$ and $\mathbb{F}(d_1, d_2)$ the ring of polynomials in $d_1$ and $d_2$, and by $\mathbb{F}[d_1, d_2]^{n\times k}$ the set of matrices of size $n \times k$ with elements in $\mathbb{F}[d_1, d_2]$.

As happens in the 1D case, the study of particular classes of matrices constitutes a fundamental tool for the analysis of 2D convolutional codes.

**Definition 1.13.** A matrix $U(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ is *unimodular* if is invertible in $\mathbb{F}[d_1,d_2]^{k\times k}$, i.e., if there exists $V(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ such that

$$V(d_1,d_2)U(d_1,d_2) = U(d_1,d_2)V(d_1,d_2) = I_k. \tag{1.4}$$

**Proposition 1.14.** *[33] Let $U(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$. The following are equivalent:*

*(i)* $U(d_1,d_2)$ *is unimodular;*

*(ii)* $\det U(d_1,d_2) = \alpha, \quad$ *where* $\quad \alpha \in \mathbb{F} \setminus \{0\}$.

**Definition 1.15.** Let $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$.

(i) $\Delta(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ is a *right-divisor* of $G(d_1,d_2)$ if

$$G(d_1,d_2) = \bar{G}(d_1,d_2)\Delta(d_1,d_2), \tag{1.5}$$

for some $\bar{G}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$.

(ii) $\Delta(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ is called a *right maximal divisor* (*rMD*) of $G(d_1,d_2)$ if (1.5) holds and

$$G(d_1,d_2) = \bar{G}(d_1,d_2)\tilde{\Delta}(d_1,d_2),$$

with $\tilde{\Delta}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ and $\bar{G}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$, implies that there exist $F(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ such that

$$\Delta(d_1,d_2) = F(d_1,d_2)\tilde{\Delta}(d_1,d_2).$$

Next we define an important class of 2D polynomial matrices, the *right-factor prime* matrices.

**Definition 1.16.** A polynomial matrix, $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$, is said to be *right-factor prime* (*rFP*) if for every factorization

$$G(d_1,d_2) = \bar{G}(d_1,d_2)\Delta(d_1,d_2), \tag{1.6}$$

$\bar{G}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ and $\Delta(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$, with $\Delta(d_1,d_2)$ unimodular.

Further properties of right-factor prime matrices are stated in the following lemma.

**Lemma 1.17.** *Let $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$.*

*(i)* $\Delta(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ *is a rMD of* $G(d_1,d_2)$ *if and only if*

$$G(d_1,d_2) = \bar{G}(d_1,d_2)\Delta(d_1,d_2),$$

*for some right-factor prime matrix* $\bar{G}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$.

*(ii) If* $G(d_1,d_2) = \bar{G}(d_1,d_2)U(d_1,d_2)$, *with* $U(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ *unimodular and* $\bar{G}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ *right-factor prime, then* $G(d_1,d_2)$ *is also right-factor prime.*

*(iii) If* $G(d_1,d_2)$ *is right-factor prime then it has full column rank.*

Consequently, if $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ is a right-factor prime matrix, then $k \leq n$.

The following proposition characterizes the class of right-factor prime 2D polynomial matrices.

**Proposition 1.18.** *[20, 33] Let* $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$, *with* $n \geq k$. *Then the following are equivalent:*

*(i)* $G(d_1,d_2)$ *is right-factor prime.*

*(ii) There exist polynomial matrices* $X_i(d_1,d_2)$ *such that*

$$X_i(d_1,d_2)G(d_1,d_2) = h_i(d_i)I_k,$$

*with* $h_i(d_i) \in \mathbb{F}[d_i] \setminus \{0\}$, *for* $i = 1,2$.

*(iii) For all* $\hat{u}(d_1,d_2) \in \mathbb{F}(d_1,d_2)^k$, $G(d_1,d_2)\hat{u}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^n$ *implies* $\hat{u}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^k$.

*(iv) The k-order minors of* $G(d_1,d_2)$ *have no common factor.*

**Corollary 1.19.** *[43] Let* $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$, *with column rank* $\bar{k}$. *There exist two polynomial matrices* $\bar{G}(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times \bar{k}}$ *rFP, and* $T(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{\bar{k}\times k}$ *with full row rank, such that*

$$G(d_1,d_2) = \bar{G}(d_1,d_2)T(d_1,d_2). \tag{1.7}$$

Note that in the case of 2D polynomial matrices, the property of being right-factor prime is not equivalent to the property of admitting a left inverse. Indeed, this fact leads to another notion that we define after the next example.

*Example* 1.20. Let us consider a polynomial matrix given by

$$G(d_1, d_2) = \begin{bmatrix} d_1 - 1 \\ d_2 - 1 \end{bmatrix}.$$

Clearly, as $d_1 - 1$ and $d_2 - 1$ do not have common factors, the matrix $G(d_1, d_2)$ is right-factor prime. In case of $G(d_1, d_2)$ admitted a left inverse, then there would exist $P(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{1\times 2}$ such that

$$P(d_1, d_2) \begin{bmatrix} d_1 - 1 \\ d_2 - 1 \end{bmatrix} = 1.$$

This would imply that, for $d_1 = d_2 = 1$,

$$P(d_1, d_2) \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1,$$

which is absurd. ◇

The subtlety lies in the fact that 2D polynomials do not admit common factors but can admit common zeros. This motivates the following definition.

**Definition 1.21.** A polynomial matrix, $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$, is said to be right-zero prime (*rZP*)if the ideal generated by the $k$-th order minors of $G(d_1, d_2)$ is the ring $\mathbb{F}[d_1, d_2]$.

This stronger notion can be characterized as follows.

**Proposition 1.22.** *[48] Let $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$, with $n \geq k$. Then the following are equivalent:*

*(i) $G(d_1, d_2)$ is right-zero prime;*

*(ii) $G(d_1, d_2)$ admits a polynomial left inverse;*

*(iii) $rank\ G(\lambda_1, \lambda_2) = k, \quad \forall (\lambda_1, \lambda_2) \in \bar{\mathbb{F}} \times \bar{\mathbb{F}}$, where $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.*

# Chapter 2

# Convolutional codes and their encoders

In this chapter, convolutional codes and convolutional encoders are defined for both 1D and 2D cases. Since a given (1D or 2D) convolutional code can be encoded by many different encoders, it becomes crucial to distinguish code properties from encoder properties. Although for the 1D case this subject is well documented in the literature, as for instance in [6, 11, 31], we have opted to present it here in detail due to its fundamental importance throughout this thesis. After this overview of known results concerning the 1D case, the 2D case is presented.

## 2.1 1D convolutional codes and their encoders

In this section we introduce convolutional codes in one-dimension and analyze several classes of encoders of such codes making use of the connections between systems theory and coding theory.

Consider one-dimensional (bilateral) sequences indexed by $\mathbb{Z}$, $\{w(i)\}_{i\in\mathbb{Z}}$, and taking values in $\mathbb{F}^n$, i.e., $w(i) \in \mathbb{F}^n$, where $\mathbb{F}$ is a field. For coding theory purposes, such sequences are identified in several ways. These sequences can be seen as elements of the set of bilateral formal power series over $\mathbb{F}^n$, denoted by $\mathcal{F}^n_{1D}$, i.e.,

$$\hat{w}(d) = \sum_{i\in\mathbb{Z}} w(i)d^i.$$

Note that $\mathcal{F}_{1D}^n$ constitutes a module over the ring $\mathbb{F}[d]$ of 1D polynomials in $d$ over $\mathbb{F}$.

Given a subset $C$ of the sequences indexed by $\mathbb{Z}$, taking values on $\mathbb{F}^n$, we denote by $\hat{C}$ the subset of $\mathcal{F}_{1D}^n$ defined by $\hat{C} = \{\hat{w} \mid w \in C\}$.

**Definition 2.1.** A *1D convolutional code* is a subset $C$ of sequences indexed by $\mathbb{Z}$ such that $\hat{C}$ is a submodule of $\mathcal{F}_{1D}^n$ which coincides with the image of $\mathcal{F}_{1D}^k$ (for some $k \in \mathbb{N}$) by a polynomial matrix $G(d)$, i.e.,

$$\hat{C} = \text{Im } G(d) = \{\hat{w}(d) \mid \hat{w}(d) = G(d)\hat{u}(d) \text{ with } \hat{u}(d) \in \mathcal{F}_{1D}^k\};$$

where **u** and **w** are the input and the output, known as *information sequences* and *codewords*, respectively; with some abuse of language we also write $C = \text{Im } G(d)$, $w$ instead of $\hat{w}$, and the same for the other variables.

In the literature, convolutional codes constituted namely by Laurent series [11] or by polynomials [39] are widely studied. In our study we consider convolutional codes constituted by bilateral sequences. In order to guarantee the completeness of our exposition, it becomes fundamental to present here some already known results concerning our case.

Note that a 1D convolutional code can always be given as the image of a full column rank polynomial operator $G(d) \in \mathbb{F}[d]^{n\times k}$.

**Definition 2.2.** Any full column rank polynomial matrix $G(d) \in \mathbb{F}[d]^{n\times k}$ such that

$$C = \text{Im } G(d)$$

is called an *encoder* of $C$; in this case $C$ is said to be of rate $k/n$.

In [26, 27], Massey and Sain recognized that two encoders can be considered *equivalent* for coding purposes if they generate the same code. The following proposition characterizes equivalent encoders of a convolutional code.

**Proposition 2.3.** *[26, 32] Let $C$ be a convolutional code of rate $k/n$ and $G_1(d) \in \mathbb{F}[d]^{n\times k}$ and $G_2(d) \in \mathbb{F}[d]^{n\times k}$ be equivalent 1D convolutional encoders. Then*

*(i) There exist two square nonsingular matrices* $P_1(d) \in \mathbb{F}[d]^{k\times k}$ *and* $P_2(d) \in \mathbb{F}[d]^{k\times k}$ *such that*

$$G_1(d)P_1(d) = G_2(d)P_2(d). \tag{2.1}$$

*(ii) If* $G_1(d)$ *is right-prime, then*

$$G_2(d) = G_1(d)P(d), \tag{2.2}$$

*for some matrix* $P(d) \in \mathbb{F}[d]^{k\times k}$.

*(iii) If* $G_1(d)$ *and* $G_2(d)$ *are both right-prime, then*

$$G_2(d) = G_1(d)U(d), \tag{2.3}$$

*for some unimodular matrix* $U(d) \in \mathbb{F}[d]^{k\times k}$.

**Remark 2.4.** *The condition (i) of the last proposition implies that convolutional codes are unique up to the post-multiplication by a square nonsingular rational matrix.*

The next proposition collects some basic results about the family of encoders of a convolutional code $C$ of rate $k/n$.

**Proposition 2.5.** *[6] Let* $C$ *be a convolutional code of rate* $k/n$. *Then*

*(i) Among all polynomial encoders of* $C$, *there always exist right-prime ones, called basic encoders.*

*(ii) Among all polynomial encoders of* $C$, *there always exist column reduced ones, called reduced encoders.*

Moreover, all the polynomial encoders of a code can be obtained from a right-prime one, by right multiplication by a polynomial matrix. Right-prime encoders are unique up to unimodular right multiplication. A convolutional code always admits polynomial encoders which are simultaneously right-prime and column reduced (cf. Definition 1.11). Such encoders are called *canonical* encoders and play an important role in coding theory specially in what regards minimality issues as we shall see latter.

Note that the column reduced encoders of $C$ do not have all the same external degree. In fact, consider two polynomial encoders $G_1(d)$ and $G_2(d)$ of $C$ with internal degrees $n_1$ and $n_2$, respectively, and such that $G_1(d)$ is right-prime but $G_2(d)$ is not. In this case one has that $n_1 < n_2$. Moreover there exist suitable unimodular matrices $U_1(d)$ and $U_2(d)$ such that

$$\tilde{G}_1(d) = G_1(d)U_1(d) \quad \text{and} \quad \tilde{G}_2(d) = G_2(d)U_2(d)$$

are column reduced encoders, with the same internal degrees as the original ones, i.e., $n_1$ and $n_2$, respectively, that coincide with the correspondent external degrees. Therefore, $G_1(d)$ and $G_2(d)$ have different external degrees.

Moreover, since canonical encoders are also basic, then from Proposition 2.3 they differ by a right unimodular factor which, by Proposition 1.12, implies that they have the same column degrees, up to a permutation. Therefore the column degrees of the canonical encoders constitute a set of invariants of the code.

Among all polynomial encoders of a convolutional code $C$, the ones with minimal external degree are the canonical encoders as the next proposition states.

**Proposition 2.6.** *[6] Let $C$ be a convolutional code of rate $k/n$ and $G(d) \in \mathbb{F}[d]^{n\times k}$ a polynomial encoder of $C$. Then $G(d)$ is canonical if and only if it has minimal external degree among all polynomial encoders of $C$.*

**Definition 2.7.** Let $C$ be a convolutional code of rate $k/n$. The (internal/external) degree of an arbitrary canonical encoder of $C$ is said to be the *degree of the code* $C$ and is denoted by $\deg C$. Moreover, the column degrees, $\phi_1, \ldots, \phi_k$, of any canonical encoder are known as *Forney indices* of $C$ and therefore their sum is the degree of the code $C$, $\deg C = \sum_{i=1}^{k} \phi_i$. The highest Forney index is said to be the *memory of the code*.

### 2.1.1 Quasi-systematic encoders

In [4], Costello noticed that there exist simple encoders that provide the information sequences by selecting some components of the correspondent codewords. Such encoders are called *systematic encoders*. In this thesis we present a similar definition.

**Definition 2.8.** An encoder $G(d) \in \mathbb{F}[d]^{n\times k}$ is said to be a *quasi-systematic* encoder if it can be reduced, up to a pre-multiplication by an invertible constant matrix, to the following structure

$$G(d) = T \begin{bmatrix} \bar{G}(d) \\ I_k \end{bmatrix}, \tag{2.4}$$

where $T \in \mathbb{F}^{n\times n}$ is invertible and $\bar{G}(d) \in \mathbb{F}[d]^{(n-k)\times k}$.

This definition is slightly different from the usual one as $T$ is any invertible constant matrix rather than a permutation matrix.

Note that not all convolutional codes admit quasi-systematic encoders. The next results establish when a 1D convolutional code admits a systematic encoder.

**Lemma 2.9.** *[31] Let $\mathcal{C}$ be a 1D convolutional code of rate $k/n$ and let $G(d)$ be a basic encoder of $\mathcal{C}$. Then $\mathcal{C}$ admits systematic encoders if and only if there exists a permutation matrix $P \in \mathbb{F}^{n\times n}$ such that*

$$\begin{bmatrix} I_k & 0 \end{bmatrix} PG(d)$$

*is unimodular.*

An immediate consequence of this lemma is the following.

**Corollary 2.10.** *Let $\mathcal{C}$ be a 1D convolutional code of rate $k/n$ and let $G(d)$ be a basic encoder of $\mathcal{C}$. Then $\mathcal{C}$ admits an encoder quasi-systematic if and only if there exists an invertible matrix $L \in \mathbb{F}^{n\times n}$ such that*

$$\begin{bmatrix} I_k & 0 \end{bmatrix} LG(d)$$

*is unimodular.*

## 2.2 2D convolutional codes and their encoders

The concept of 2D convolutional code has been introduced by extending, in a natural way, the notion of convolutional code for the 1D case.

Let us consider 2D convolutional codes constituted by sequences indexed by $\mathbb{Z}^2$ and taking values in $\mathbb{F}^n$, where $\mathbb{F}$ is a field. Such sequences $\{w(i,j)\}_{(i,j)\in\mathbb{Z}^2}$ can be represented by bilateral formal power series

$$\hat{w}(d_1,d_2) = \sum_{(i,j)\in\mathbb{Z}^2} w(i,j)d_1^i d_2^j.$$

For $n \in \mathbb{N}$, the set of bilateral formal power series over $\mathbb{F}^n$ is denoted by $\mathcal{F}_{2D}^n$. This set is a module over the ring $\mathbb{F}[d_1,d_2]$ of 2D polynomials over $\mathbb{F}$.

Given a subset $C$ of sequences indexed by $\mathbb{Z}^2$, taking values on $\mathbb{F}^n$, we denote by $\hat{C}$ the subset of $\mathcal{F}_{2D}^n$ defined by $\hat{C} = \{\hat{w} \mid w \in C\}$, $w$ instead of $\hat{w}$, and the same for the other variables.

**Definition 2.11.** A *2D convolutional code* is a subset $C$ of sequences indexed by $\mathbb{Z}^2$ such that $\hat{C}$ is a submodule of $\mathcal{F}_{2D}^n$ which coincides with the image of $\mathcal{F}_{2D}^k$ (for some $k \in \mathbb{N}$) by a polynomial matrix $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$, i.e.,

$$\begin{aligned}\hat{C} &= \text{Im } G(d_1,d_2)\\ &= \{\hat{w}(d_1,d_2) \mid \hat{w}(d_1,d_2) = G(d_1,d_2)\hat{u}(d_1,d_2) \text{ with } \hat{u}(d_1,d_2) \in \mathcal{F}_{2D}^k\};\end{aligned}$$

with some abuse of language we also write $C = \text{Im } G(d_1,d_2)$.

It follows as a consequence of [Theorem 2.2, [23]] that a 2D convolutional code can always be given as the image of a full column rank polynomial matrix $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$.

**Definition 2.12.** Any full column rank matrix $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ such that $C = \text{Im } G(d_1,d_2)$ is called an *encoder* of $C$.

Note that this definition of encoder is slightly different from the one in [10] where non full column rank 2D polynomial matrices are allowed as encoders. However, our definition is motivated by the fact that only full column rank encoders are relevant for the purpose of obtaining minimal realizations of a code.

As happens in the 1D case, a 2D convolutional code can be generated by different encoders.

**Definition 2.13.** Two encoders, $G_1(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ and $G_2(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$, are said to be *equivalent* if they generate the same code, i.e., if

$$\text{Im } G_1(d_1,d_2) = \text{Im } G_2(d_1,d_2).$$

This means that two matrices $G_1(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ and $G_2(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ are equivalent encoders if the $\mathcal{F}_{2D}^n$- modules generated by the columns of $G_1(d_1,d_2)$ and $G_2(d_1,d_2)$ coincide. As a consequence it follows the next characterization of equivalent encoders .

**Proposition 2.14.** *[10] Let $G_1(d_1,d_2),\ G_2(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ be (equivalent) 2D convolutional encoders. Then*

*(i) There exist two square nonsingular matrices $P_1(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$ and $P_2(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$, such that*

$$G_1(d_1,d_2)P_1(d_1,d_2) = G_2(d_1,d_2)P_2(d_1,d_2).$$

*(ii) If $G_1(d_1,d_2)$ is right-factor prime, then*

$$G_2(d_1,d_2) = G_1(d_1,d_2)P(d_1,d_2),$$

*for some 2D matrix $P(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$.*

*(iii) If $G_1(d_1,d_2)$ and $G_2(d_1,d_2)$ are both right-factor prime, then*

$$G_2(d_1,d_2) = G_1(d_1,d_2)U(d_1,d_2),$$

*for some 2D unimodular matrix $U(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{k\times k}$.*

It follows from (i) in the previous proposition that

$$G_1(d_1,d_2) = G_2(d_1,d_2)U_2(d_1,d_2) \quad \text{and} \quad G_2(d_1,d_2) = G_1(d_1,d_2)U_1(d_1,d_2),$$

with $U_2(d_1,d_2) = P_2(d_1,d_2)P_1^{-1}(d_1,d_2)$ and $U_1(d_1,d_2) = P_1(d_1,d_2)P_2^{-1}(d_1,d_2)$, i.e., as happens in the 1D case, the 2D convolutional encoders are unique up to the post-multiplication by a square nonsingular 2D rational matrix.

As a consequence, a 2D convolutional code always admits right-factor prime encoders. However, is not true that it always admits right-zero prime ones.

*Example* 2.15. Recall the Example 1.20

$$G(d_1, d_2) = \begin{bmatrix} d_1 - 1 \\ d_2 - 1 \end{bmatrix}.$$

Clearly, as $d_1 - 1$ and $d_2 - 1$ do not have common factors, the matrix $G(d_1, d_2)$ is right-factor prime. However, since its maximal order minors have a common zero for $d_1 = d_2 = 1$, $G(d_1, d_2)$ does not admit a left polynomial inverse and therefore is not right-zero prime. $\diamond$

# Chapter 3

# The realization problem

In this chapter we start by introducing the notions of realization of an encoder and of the corresponding convolutional code. Moreover, it is our purpose to analyze the realization problem for both one and two-dimensional convolutional codes starting from their encoders.

## 3.1 The one-dimensional case

In this section we consider state-space models. Depending on what type of situation we are interested in, these models can be viewed from different perspectives, namely as realizations of input/output relations (corresponding to encoders) or as realizations of output behaviors (corresponding to codes). The minimality of such representations is also investigated and an algorithm to obtain a minimal realization of a code starting from a minimal realization of one of its encoders is presented.

### 3.1.1 Realizations of 1D encoders

A discrete-time 1D state-space model is a description of a linear, discrete and time-invariant 1D system through equations of the form:

$$\begin{cases} \sigma x(t) = Ax(t) + Bu(t) \\ w(t) = Cx(t) + Du(t), \end{cases} \tag{3.1}$$

where $A$, $B$, $C$ and $D$ are matrices over $\mathbb{F}$ of size $m \times m$, $m \times k$, $n \times m$ and $n \times k$, respectively; $\sigma x(t) = x(t+1)$, for all $t \in \mathbb{Z}$, $u$ is the input-variable, $w$ is the output-variable and $x$ is the state-variable. The system described by (3.1) will be denoted by $\Sigma^{1D}(A, B, C, D)$, and its dimension is defined to be the dimension of the state space, i.e., $m$.

Some relevant definitions and results concerning this type of models are given in the Appendix A.

**Definition 3.1.** $\Sigma^{1D}(A, B, C, D)$ is said to be a *realization of the 1D encoder* $G(d) \in \mathbb{F}[d]^{n \times k}$ if

$$G(d) = C(I_m - Ad)^{-1}Bd + D.$$

Under the light of the behavioral approach, this is equivalent to say that $\Sigma^{1D}(A, B, C, D)$ is a realization of an encoder $G(d)$ if the behavior

$$\mathcal{B}_{(u,w)} = \{(u, w) \mid \hat{w}(d) = G(d)\hat{u}(d)\}$$

coincides with the set

$$\{(u, w) \mid \exists\ x \text{ such that } (u, x, w) \text{ satisfies (3.1)}\}.$$

In this case we write $\Sigma^{1D}(A, B, C, D) = \Sigma^{1D}(G)$.

Note that the set $\mathcal{B}_{(u,w)}$ is what is known in the behavioral approach to systems and control [46] as the (external) input/output behavior associated with (3.1).

#### 3.1.1.1 Minimal realizations of 1D encoders

A polynomial encoder $G(d) \in \mathbb{F}[d]^{n \times k}$ admits many realizations with possibly different dimensions. Efficiency leads to focusing on obtaining realizations of minimal dimension.

**Definition 3.2.** Let $G(d) \in \mathbb{F}[d]^{n \times k}$. $\Sigma^{1D}(A, B, C, D)$ is said to be a *minimal realization* of $G(d)$ if no other realization of $G(d)$ has smaller dimension, i.e., if the size of the state $x$ is minimal among all the realizations of $G(d)$. The minimal dimension of a realization of $G(d)$ is called the *McMillan degree* of $G(d)$ and is represented by $\mu(G)$.

It is well known that the minimal realizations of an encoder $G(d) \in \mathbb{F}[d]^{n\times k}$ are characterized by being simultaneously observable and controllable[1] (see Appendix A).

The next proposition characterizes the McMillan degree of a general polynomial matrix, and in particular of an encoder. A similar result has been proved in [9, 18], in a different context, using different tools.

**Proposition 3.3.** *Let $G(d) \in \mathbb{F}[d]^{n\times k}$. Then the McMillan degree of $G(d)$ is given by*

$$\mu(G) = \text{int deg} \begin{bmatrix} G(d) \\ I_k \end{bmatrix}.$$

*Proof.* Let $N(d) \in \mathbb{F}[d]^{n\times k}$ and $D(d) \in \mathbb{F}[d]^{k\times k}$ invertible be such that $G(d) = N(d)D(d)^{-1}$ with

$$\begin{bmatrix} N(d) \\ D(d) \end{bmatrix} \tag{3.2}$$

right prime and column reduced. It is well known that the McMillan degree of $G(d)$ is $\text{ext deg} \begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$, see for example [9, 18]. Since $\begin{bmatrix} G(d) \\ I_k \end{bmatrix}$ and $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ are right prime and

$$\begin{bmatrix} G(d) \\ I_k \end{bmatrix} D(d) = \begin{bmatrix} N(d) \\ D(d) \end{bmatrix},$$

it follows that $D(d)$ is unimodular and hence

$$\text{int deg} \begin{bmatrix} N(d) \\ D(d) \end{bmatrix} = \text{int deg} \begin{bmatrix} G(d) \\ I_k \end{bmatrix}.$$

[1] Recall that $\Sigma(A,B,C,D)$ of dimension $m$ is controllable if and only if rank $\begin{bmatrix} B \mid AB \mid \cdots \mid A^{m-1}B \end{bmatrix} = m$, or, equivalently, if and only if rank $\begin{bmatrix} \lambda I_m - A \mid B \end{bmatrix} = m, \quad \forall \lambda \in \bar{\mathbb{F}}$. $\Sigma(A,B,C,D)$ is observable if and only if rank $\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{m-1} \end{bmatrix} = m$, or, equivalently, if and only if rank $\begin{bmatrix} \lambda I_m - A \\ C \end{bmatrix} = m, \quad \forall \lambda \in \bar{\mathbb{F}}$. Here $\bar{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$.

Because $\begin{bmatrix} N(d) \\ D(d) \end{bmatrix}$ is column reduced, we have that

$$\text{ext deg} \begin{bmatrix} N(d) \\ D(d) \end{bmatrix} = \text{int deg} \begin{bmatrix} G(d) \\ I_k \end{bmatrix}. \qquad \square$$

Observe that, from the proposition above together with the definition of internal degree, it follows that the McMillan degree of a polynomial matrix $G(d)$ is the maximum degree of its minors.

As we referred before, in general a realization of an encoder is not unique. Nevertheless, a minimal one is unique up to a change of basis on the state-space as next proposition states. Therefore we say that minimal realizations of an encoder (and equivalently of an input/output behaviour) are equivalent.

**Proposition 3.4.** *[19] Let $\Sigma^{1D}(A,B,C,D)$ and $\bar{\Sigma}^{1D}(\bar{A},\bar{B},\bar{C},\bar{D})$ be two minimal realizations of an encoder $G(d)$. Then, there exists a unique invertible matrix $T$ such that*

$$\bar{A} = T^{-1}AT,\ \bar{B} = T^{-1}B,\ \bar{C} = CT \text{ and } \bar{D} = D. \tag{3.3}$$

There exist several algorithms in the literature to obtain minimal realizations of polynomial encoders [9, 18]. The following procedure is an example of an algorithm of this type.

**Algorithm 3.5.** *[9] Given a polynomial matrix $G(d) \in \mathbb{F}[d]^{n\times k}$, let $U(d)$ be a unimodular matrix such that*

$$\begin{bmatrix} \bar{G}(d) \\ U(d) \end{bmatrix} = \begin{bmatrix} G(d) \\ I_k \end{bmatrix} U(d) \tag{3.4}$$

*is column reduced with column degrees given by $\ell_1,\ldots,\ell_k$, respectively.*

*Let us assume that $\ell_i > 0$ for $i = 1,\ldots,k$ and let $m = \ell_1 + \ell_2 + \cdots + \ell_k$.*

***Step 1*** *Rewrite $G(d) = \bar{G}(d)U(d)^{-1}$ as*

$$G(d) = \bar{G}(0)U(0)^{-1} + \tilde{G}(d)U(d)^{-1}, \tag{3.5}$$

*where $\tilde{G}(d) = \bar{G}(d) - \bar{G}(0)U(0)^{-1}U(d)$ and $\begin{bmatrix} \tilde{G}(d) \\ U(d) \end{bmatrix}$ is column reduced with the same column degrees as the matrix in (3.4). In order to obtain a minimal realization of $G(d)$,*

*take*

$$D = \bar{G}(0)U(0)^{-1} \tag{3.6}$$

*and reduce the problem to finding a realization of* $\tilde{G}(d)U(d)^{-1}$.

***Step 2*** *Denote by* $M_i$ *the* $\ell_i \times \ell_i$ *nilpotent Jordan block matrix given by*

$$M_i = \begin{bmatrix} 0 & & & \\ 1 & 0 & & \\ & \ddots & \ddots & \\ & & 1 & 0 \end{bmatrix}, \tag{3.7}$$

*and define the matrices*

$$\overline{M} = M_{\ell_1} \oplus M_{\ell_2} \oplus \cdots \oplus M_{\ell_k},$$

*and*

$$\overline{B} = \begin{bmatrix} e_1 & e_{1+\ell_1} & \cdots & e_{1+\ell_1+\cdots+\ell_{k-1}} \end{bmatrix},$$

*of dimension* $m \times m$ *and* $m \times k$*, respectively, where the notation* $M \oplus N$ *represents the block diagonal matrix with diagonal blocks* $M$ *and* $N$.

*It is clear that the matrix* $X(d) = (I_m - \bar{M}d)^{-1}\bar{B}d$ *admits the following structure:*

$$X(d) = \begin{bmatrix} d & & & \\ d^2 & & & \\ \vdots & & & \\ d^{\ell_1} & & & \\ & d & & \\ & d^2 & & \\ & \vdots & & \\ & d^{\ell_2} & & \\ & & \ddots & \\ & & & d \\ & & & d^2 \\ & & & \vdots \\ & & & d^{\ell_k} \end{bmatrix} \tag{3.8}$$

*Therefore, each row of* $\tilde{G}(d)$ *can be written as a linear combination of the rows of* $X(d)$. *Define* $C \in \mathbb{F}^{n\times m}$ *such that*

$$\tilde{G}(d) = CX(d). \tag{3.9}$$

***Step 3*** *Note that as $U(d)$ is unimodular and the column degrees are lower or equal that $\ell_1, \ldots, \ell_k$ it is always possible to write $U(d) = U(0)(I_k - \bar{A}X(d))$, for a suitable $\bar{A} \in \mathbb{F}^{k\times m}$, where $I_k - \bar{A}X(d)$ is nonsingular. Define*

$$A = \bar{M} + \bar{B}\bar{A} \quad \textit{and} \quad B = \bar{B}U(0)^{-1}. \tag{3.10}$$

It can be easily proven that $(I_m - Ad)X(d) = \bar{B}d(I_m - \bar{A}X(d))$ which implies

$$\bar{G}(d)U(d)^{-1} = C(I_m - Ad)^{-1}Bd.$$

Thus (3.6), (3.9) and (3.10) provide an $m$-dimensional state-space realization of the $G(d)$.

If $\ell_i = 0$, for some $i$, the procedure is the same as above; however the $i$th column in $\bar{B}$ and in $X(d)$ has to be zero, and the $i$th diagonal block $M_{\ell_i}$ is empty.

It is worth mentioning that canonical encoders have minimal McMillan degree among all the encoders of a 1D convolutional code as the following proposition states.

**Proposition 3.6.** *[9, 12] Canonical encoders of a 1D convolutional code $C$ have minimal McMillan degree among all encoders of the code.*

*Proof.* Let $G(d)$ be an encoder of $C$ and $G_c(d)$ an equivalent canonical encoder. Then

$$G(d) = G_c(d)\Delta(d),$$

for some $\Delta(d) \in \mathbb{F}[d]^{k\times k}$.

Let $U(d) \in \mathbb{F}[d]^{k\times k}$ be a unimodular matrix such that

$$\begin{bmatrix} G(d) \\ I_k \end{bmatrix} U(d),$$

is column reduced. Then,

$$\begin{aligned}
\text{int deg}\begin{bmatrix} G(d) \\ I_k \end{bmatrix} &= \text{int deg}\begin{bmatrix} G_c(d)\Delta(d) \\ I_k \end{bmatrix} = \text{int deg}\begin{bmatrix} G_c(d)\Delta(d)U(d) \\ U(d) \end{bmatrix} \\
&= \text{ext deg}\begin{bmatrix} G_c(d)\Delta(d)U(d) \\ U(d) \end{bmatrix} \\
&\geq \text{ext deg}(G_c(d)\Delta(d)U(d)) \\
&\geq \text{int deg}(G_c(d)\Delta(d)U(d)) \\
&\geq \text{int deg}(G_c(d)) = \text{ext deg}(G_c(d)) \\
&= \text{ext deg}\begin{bmatrix} G_c(d) \\ I_k \end{bmatrix} = \text{int deg}\begin{bmatrix} G_c(d) \\ I_k \end{bmatrix}.
\end{aligned}$$

□

From the proof of the proposition above, it follows immediately that if $G(d)$ is an encoder of a 1D convolutional code which is not right-prime, then its McMillan degree is greater than the McMillan degree of an equivalent canonical encoder.

### 3.1.2 Realizations of 1D convolutional codes

In this section we consider realizations of 1D convolutional codes.

**Definition 3.7.** $\Sigma^{1D}(A,B,C,D)$ is said to be a *realization* of the 1D convolutional code $\mathcal{C}$ if the corresponding $w-$ behavior

$$\mathcal{B}_w = \{w \mid \mathbb{Z} \to \mathbb{F}^n : \exists\, x,u \text{ such that } (u,x,w) \text{ satisfies (3.1)}\}$$

coincides with $\mathcal{C}$, that is, $\mathcal{B}_w = \mathcal{C}$.

This is denoted by $\Sigma^{1D}(A,B,C,D) = \Sigma^{1D}(\mathcal{C})$.

It is not difficult to see that a realization of an encoder of a convolutional code is also a realization of the corresponding code, however the converse is not true.

It turns out that a code $\mathcal{C}$ can be regarded as a behavior, the main object of study of the already mentioned behavioral approach developed by J.C. Willems [46]. The behaviors corresponding to 1D convolutional codes constitute a particular class of behaviors, known as

controllable behaviors, that are precisely sets of trajectories (sequences) that constitute the image of a polynomial shift-operator (in coding language, the encoder). Within the behavioral approach, a particular type of state-space representations for a behavior $\mathcal{B}$ have been introduced, called state/driving-variable (s/dv) representations, whose input is an auxiliary variable (the driving-variable); the behavior $\mathcal{B}$ corresponds to the output behavior of the s/dv model. Thus, the realizations of a code $C$ are nothing else than s/dv realizations of the controllable behavior $\mathcal{B} = C$.

#### 3.1.2.1 Minimal realizations of 1D convolutional codes

**Definition 3.8.** $\Sigma^{1D}(C)$ is said to be a *minimal realization* of the 1D convolutional code $C$ if the size of $(x,u)$ is minimal among all the realizations of $C$. The minimal size of $(x,u)$ is denoted by $\eta(C)$.

A complete characterization for the minimality of code realizations is given by the conditions of minimality of 1D s/dv realizations for controllable behaviors that can be derived from [Theorem 4.2, [46]], and are stated as follows using the terminology of codes.

**Theorem 3.9.** *[Theorem 4.2, [46]] A realization $\Sigma^{1D}(A,B,C,D)$ of a convolutional code $C$ is minimal if and only if the following conditions are satisfied:*

*(i)* $\begin{bmatrix} B \\ D \end{bmatrix}$ *has full column rank;*

*(ii)* $(A,B)$ *is a controllable pair;*

*(iii)* $\ker D \subseteq \ker B$*, i.e., there exists a matrix* $L \in \mathbb{F}^{m\times n}$ *such that* $B = LD$*;*

*(iv) Let $L$ be as in (iii), and let $\Lambda \in \mathbb{F}^{(n-k)\times n}$ be a minimal left-annihilator (mla)[2] of $D$. Then the pair $(A - LC, \Lambda C)$ is observable.*

**Remark 3.10.** *Note that (i) and (iii) are equivalent to (i') –D has full column rank– and (iii).*

The next example shows that a minimal realization of an encoder $G(d)$ of a code $C$ is not necessarily a minimal realization of the code $C$.

[2] $\Lambda$ is a *mla* of $D$ if $\Lambda D = 0$ and for all $\Lambda^*$ such that $\Lambda^* D = 0$ there exists $\tilde{\Lambda}$ satisfying $\Lambda^* = \tilde{\Lambda}\Lambda$.

*Example* 3.11. Consider the following 1D polynomial encoder of a code $C$

$$G(d) = \begin{bmatrix} 1 + d - d^3 & -1 + d^3 \\ d + d^2 - d^3 & -1 - d^2 + d^3 \\ d + d^2 & -1 - d - d^2 \end{bmatrix}.$$

It can be easily checked that $\Sigma^{1D}(A, B, C, D)$ with

$$A = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & -1 \\ 0 & 0 \\ 0 & -1 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & -1 \\ 1 & 1 & -1 \\ 1 & 1 & 0 \end{bmatrix} \quad \text{and} \quad D = \begin{bmatrix} 1 & -1 \\ 0 & -1 \\ 0 & -1 \end{bmatrix}$$

is a realization of $G(d)$ which is controllable and observable and therefore is minimal.

However $\Sigma^{1D}(A, B, C, D)$ is not a minimal realization of $C$, as not all the conditions of Theorem 3.9 are satisfied. Indeed, condition (iii) is fulfilled for

$$L = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

however, considering the minimal left-annihilator $\Lambda = \begin{bmatrix} 0 & 1 & -1 \end{bmatrix}$ of $D$, we have that

$$A - LC = \begin{bmatrix} -1 & 0 & 1 \\ 1 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix} \quad \text{and} \quad \Lambda C = \begin{bmatrix} 0 & 0 & -1 \end{bmatrix},$$

are such that the pair $(A - LC, \Lambda C)$ is not observable.

Let us consider an equivalent encoder

$$\bar{G}(d) = G(d)U(d)^{-1},$$

where $\bar{G}(d) = \begin{bmatrix} 1 + d & -d \\ d & -d + 1 \\ d & 1 \end{bmatrix}$ and $U(d)^{-1} = \begin{bmatrix} 1 & -1 \\ d^2 & -1 - d^2 \end{bmatrix}$. Then $\bar{\Sigma}^{1D}(\bar{A}, \bar{B}, \bar{C}, \bar{D})$ with

$$\bar{A} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} 1 & -1 \\ 1 & -1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \bar{D} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix}$$

is a minimal realization of $\bar{G}(d)$. Moreover, it is easy to see that such realization satisfies conditions (i), (ii) and (iii) for

$$L = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

With respect to condition (iv), considering the minimal left-annihilator $\Lambda = \begin{bmatrix} 0 & -1 & 1 \end{bmatrix}$ of $\bar{D}$, we have that

$$\bar{A} - L\bar{C} = \begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix} \quad \text{and} \quad \Lambda\bar{C} = \begin{bmatrix} 0 & 1 \end{bmatrix},$$

are such that the pair $(\bar{A} - L\bar{C}, \Lambda\bar{C})$ is observable. Hence, $\bar{\Sigma}^{1D}(\bar{G})$ is a minimal realization of the convolutional code $C$. ◇

Minimal encoders are defined as the ones for which a minimal realization is also minimal as a code realization; this is formalized in the following definition.

**Definition 3.12.** Let $C \subset \mathcal{F}_{1D}^n$ be a convolutional code and $G(d) \in \mathbb{F}[d]^{n\times k}$ an encoder of $C$. $G(d)$ is said to be a *minimal encoder* of $C$ if

$$\mu(G) + k = \eta(C).$$

Note that it follows from Proposition 3.6 that canonical encoders are minimal.

**Remark 3.13.** *The situation illustrated in the previous example is due to the fact that when realizing an input/output operator (encoder) $G(d)$ one has no freedom in performing transformations in the input. This restriction is not present in the realization of the corresponding output behavior (code), where the input-variables may be transformed. Therefore, given a minimal realization of a non-minimal encoder $G(d)$, it is still possible to reduce its dimension in order to have a minimal realization of the corresponding code.*

The following procedure shows precisely how to obtain a minimal realization

$$\tilde{\Sigma}^{1D}(C) = \tilde{\Sigma}^{1D}(\tilde{A}, \tilde{B}, \tilde{C}, \tilde{D})$$

of a code $C$ by performing operations and reducing the number of variables in a minimal realization $\Sigma^{1D}(G) = \Sigma^{1D}(A, B, C, D)$ of a corresponding encoder $G(d)$.

Let us consider $\Sigma^{1D}(A,B,C,D)$ a minimal realization of $G(d)$. Then

$$\begin{aligned} G(d) &= C(I_m - Ad)^{-1}Bd + D \\ &= \left[\begin{array}{c|c} C(I_m - Ad)^{-1}d & I_n \end{array}\right] \begin{bmatrix} B \\ D \end{bmatrix}. \end{aligned}$$

Since encoders have full column rank, clearly $\begin{bmatrix} B \\ D \end{bmatrix}$ must have full column rank and hence condition (i) of Theorem 3.9 is satisfied. Moreover, the minimality of $\Sigma^{1D}(A,B,C,D)$ as realization of the encoder $G(d)$ implies the controllability of the pair $(A,B)$. Thus, a minimal realization of the encoder $G(d)$ satisfies condition (ii) of Theorem 3.9.

Suppose now that condition (iii) of the Theorem 3.9 is not satisfied i.e., $\ker D \not\subseteq \ker B$. Then we can suppose, without loss of generality, that

$$D = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \text{ and } B = \begin{bmatrix} B_1 & B_2 \end{bmatrix}, \tag{3.11}$$

with $B_2 = \begin{bmatrix} 0 \\ S \end{bmatrix}$ full column rank of size $m \times (k-r)$, where $S$ is a square invertible matrix of size $k-r$, and $B_1 = \begin{bmatrix} B_{11} \\ B_{21} \end{bmatrix}$ of size[3] $m \times r$.
Therefore, (3.1) is of the form:

$$\begin{cases} \sigma x_1 = A_{11}x_1 + A_{12}x_2 + B_{11}u_1 & \text{(3.12a)} \\ \sigma x_2 = A_{21}x_1 + A_{22}x_2 + B_{21}u_1 + Su_2 & \text{(3.12b)} \\ w_1 = C_{11}x_1 + C_{12}x_2 + Iu_1 & \text{(3.12c)} \\ w_2 = C_{21}x_1 + C_{22}x_2, & \text{(3.12d)} \end{cases}$$

where the variables $x$, $u$ and $w$ have been partitioned according to the given matrix partitions.

[3]If this is not the case, changes of coordinates in the $u$, $x$, $w$ spaces allow bringing $D$ and $B$ to the desired form. The coordinate change in the $w$ space modifies the code under consideration, but can be reversed at the end of the reasoning that will be presented.

Equations (3.12a)–(3.12d) show that $x_2$ is a free variable. Indeed, given $x_2$ and $u_1$, it is possible to find $x_1$, $w_1$ and $w_2$ such that equations (3.12a), (3.12c) and (3.12d) are satisfied. Moreover, since $S$ is invertible, there exists $u_2$ such that (3.12b) holds. Therefore, this latter equation can be eliminated from the description of the code $C$, and $x_2$ can assume the role of a driving variable. This means that

$$\begin{cases} \sigma x_1 = A_{11}x_1 + \bar{B}\bar{u} \\ w = C_1 x_1 + \bar{D}\bar{u}, \end{cases} \tag{3.13}$$

with $\bar{B} = \begin{bmatrix} A_{12} & B_{11} \end{bmatrix}$, $\bar{u} = \begin{bmatrix} x_2 \\ u_1 \end{bmatrix}$, $C_1 = \begin{bmatrix} C_{11} \\ C_{21} \end{bmatrix}$ and $\bar{D} = \begin{bmatrix} C_{12} & I \\ C_{22} & 0 \end{bmatrix}$ is still a realization of the code with smaller dimension than the initial one (recall that the dimension of a code realization is defined as the size of the joint state and driving-variable vector).

Note that the new system obtained in (3.13) still satisfies the condition (ii) of Theorem 3.9 since if the pair

$$(A, B) = \left( \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \begin{bmatrix} B_{11} & 0 \\ B_{21} & S \end{bmatrix} \right)$$

is controllable, then the pair

$$(A_{11}, \bar{B}) = \left( A_{11}, \begin{bmatrix} A_{12} & B_{11} \end{bmatrix} \right)$$

is also controllable. Indeed the controllability condition

$$\operatorname{rank} \left[ \lambda I_m - A \;\middle|\; B \right] = m, \quad \forall \lambda \in \bar{\mathbb{F}},$$

becomes

$$\operatorname{rank} \begin{bmatrix} \lambda I_{m_1} - A_{11} & -A_{12} & B_{11} & 0 \\ -A_{21} & \lambda I_{m_2} - A_{22} & B_{21} & S \end{bmatrix} = m_1 + m_2 = m, \quad \forall \lambda \in \bar{\mathbb{F}},$$

where $m_1 = m - (k - r)$ and $m_2 = k - r$, which implies that

$$\operatorname{rank} \left[ \lambda I_{m_1} - A_{11} \;\middle|\; A_{12} \;\middle|\; B_{11} \right] = \operatorname{rank} \left[ \lambda I_{m_1} - A_{11} \;\middle|\; -A_{12} \;\middle|\; B_{11} \right] = m_1,$$

meaning that $(A_{11}, \bar{B})$ is a controllable pair.

Moreover, in case $\begin{bmatrix} \bar{B} \\ \bar{D} \end{bmatrix}$ is not full column rank, there exists an invertible matrix $T$ such that

$$\begin{bmatrix} \bar{B} \\ \bar{D} \end{bmatrix} T = \begin{bmatrix} \bar{\bar{B}} & 0 \\ \bar{\bar{D}} & 0 \end{bmatrix},$$

with $\begin{bmatrix} \bar{\bar{B}} \\ \bar{\bar{D}} \end{bmatrix}$ full column rank. Partitioning $T^{-1}\bar{u}$ accordingly as $T^{-1}\bar{u} = \begin{bmatrix} \bar{\bar{u}} \\ \tilde{u} \end{bmatrix}$, equations (3.13) become

$$\begin{cases} \sigma x_1 = A_{11} x_1 + \bar{\bar{B}}\bar{\bar{u}} \\ w = C_1 x_1 + \bar{\bar{D}}\bar{\bar{u}}, \end{cases} \tag{3.14}$$

which again yields a realization of the code $C$ with smaller dimension as the previous one, that satisfies again condition (i) of Theorem 3.9.

Since

$$\left[\lambda I_{m_1} - A_{11} \;\middle|\; \bar{\bar{B}} \;\middle|\; 0\right] = \left[\lambda I_{m_1} - A_{11} \;\middle|\; \bar{B}T\right] = \left[\lambda I_{m_1} - A_{11} \;\middle|\; \bar{B}\right] \begin{bmatrix} I & 0 \\ 0 & T \end{bmatrix},$$

where $I$ denotes the identity matrix of suitable size, and

$$\begin{aligned} \operatorname{rank} \left[\lambda I_{m_1} - A_{11} \;\middle|\; \bar{\bar{B}}\right] &= \operatorname{rank} \left[\lambda I_{m_1} - A_{11} \;\middle|\; \bar{\bar{B}} \;\middle|\; 0\right] \\ &= \operatorname{rank} \left[\lambda I_{m_1} - A_{11} \;\middle|\; \bar{B}\right], \end{aligned}$$

the controllability of the pair $(A_{11}, \bar{B})$ implies that the pair $(A_{11}, \bar{\bar{B}})$ is controllable, and the realization (3.14) also satisfies condition (ii) of Theorem 3.9.

In case this realization does not satisfy condition (iii) of Theorem 3.9, the procedure can be restarted and repeated, yielding successive realizations of the code with smaller dimension, till a realization of the code is obtained that simultaneously satisfies conditions (i), (ii) and (iii). To avoid introducing too much notation, this realization will be again denoted by $\Sigma^{1D}(A, B, C, D)$ (as the original one).

Suppose now that $\Sigma^{1D}(A,B,C,D)$ does not satisfy condition (iv) of Theorem 3.9. From (3.1) and since the condition (iii) is satisfied we have that

$$\begin{cases} \sigma x = Ax + LDu \\ w = Cx + Du, \end{cases} \tag{3.15}$$

Since $Du = w - Cx$ implies $LDu = Lw - LCx$, (3.15) is equivalent to

$$\begin{cases} \sigma x = (A - LC)x + Lw \\ w = Cx + Du, \end{cases} \tag{3.16}$$

Let $\Lambda$ be a *mla* of $D$. Then, there exists a matrix $X$ such that $V = \begin{bmatrix} X \\ \Lambda \end{bmatrix}$ is invertible and $VD = \begin{bmatrix} X \\ \Lambda \end{bmatrix} D = \begin{bmatrix} I_k \\ 0 \end{bmatrix}$. Let $\bar{w} = Vw = \begin{bmatrix} X \\ \Lambda \end{bmatrix} w$ be partitioned in the obvious way as $\bar{w} = \begin{bmatrix} \bar{w}_1 \\ \bar{w}_2 \end{bmatrix} = \begin{bmatrix} Xw \\ \Lambda w \end{bmatrix}$. It follows from (3.16) that

$$\begin{cases} \sigma x = (A - LC)x + LV^{-1}\bar{w} \\ \bar{w}_1 = XCx + u \\ \bar{w}_2 = \Lambda Cx, \end{cases} \tag{3.17}$$

The second equation of (3.17) shows that $\bar{w}_1$ is a free variable, which may be taken as a new driving-variable, replacing $u$. Letting $V^{-1}$ be suitably partitioned as $\begin{bmatrix} R & Q \end{bmatrix}$, this yields

$$\begin{cases} \sigma x = (A - LC)x + LR\bar{w}_1 + LQ\bar{w}_2 \\ \bar{w}_2 = \Lambda Cx. \end{cases} \tag{3.18}$$

Since $\Sigma^{1D}(A,B,C,D)$ does not satisfy condition (iv) of Theorem 3.9, the pair $(A-LC,\Lambda C)$ is not observable; thus by reducing equations (3.18) to the Kalman observability decomposition form through a coordinate change in the state-space, and eliminating the nonobservable states (see Appendix A) we obtain a description

$$\begin{cases} \sigma \bar{x} = \bar{A}\bar{x} + \bar{B}_1\bar{w}_1 + \bar{B}_2\bar{w}_2 \\ \bar{w}_2 = \bar{C}\bar{x}, \end{cases} \tag{3.19}$$

for the same set of $(\bar{w}_1, \bar{w}_2)$ trajectories as (3.18), where the size of the state $\bar{x}$ is smaller than the one of $x$. Equations (3.19) can still be written as

$$\begin{cases} \sigma\bar{x} = (\bar{A} + \bar{B}_2\bar{C})\bar{x} + \bar{B}_1\bar{u}_1 \\ \bar{w}_1 = \bar{u}_1 \\ \bar{w}_2 = \bar{C}\bar{x}, \end{cases} \tag{3.20}$$

which, by noting that

$$w = V^{-1}\bar{w} = \begin{bmatrix} R & Q \end{bmatrix} \begin{bmatrix} \bar{w}_1 \\ \bar{w}_2 \end{bmatrix} = R\bar{w}_1 + Q\bar{w}_2 = R\bar{u}_1 + Q\bar{C}\bar{x}$$

finally yields:

$$\begin{cases} \sigma\bar{x} = \bar{\bar{A}}\bar{x} + \bar{B}_1\bar{u}_1 \\ w = \bar{\bar{C}}\bar{x} + \bar{D}\bar{u}_1, \end{cases} \tag{3.21}$$

with $\bar{\bar{A}} = \bar{A} + \bar{B}_2\bar{C}$, $\bar{\bar{C}} = Q\bar{C}$ and $\bar{D} = R$.

This is a state-space realization for the same code as $\Sigma^{1D}$(A,B,C,D), but with smaller dimension.

If one of the conditions of Theorem 3.9 is not satisfied by the realization $\Sigma^{1D}(\bar{\bar{A}}, \bar{B}, \bar{\bar{C}}, \bar{D})$, then one can perform the relevant steps described above, reducing each time the dimension of the code realization. In this way a minimal state/driving-variable realization of the initial code is obtained in a finite number of steps.

It is however worth mentioning the following. As we have just seen, the state-space system that satisfies all conditions of Theorem 3.9 obtained by this procedure (and that we once more denoted by $\Sigma^{1D}(A, B, C, D)$, with dimension $m$, by resetting the notation) is a minimal realization of $C$. Nevertheless it can happen that $C(I_m - Ad)^{-1}Bd + D$ is no longer polynomial and hence is not an encoder of $C$. In that case, due to the controllability of the pair $(A, B)$, there exists a matrix $K$ of suitable size such that $A - BK$ has only zero eigenvalues, and is therefore nilpotent. This implies that the square $(m \times m)$ polynomial matrix $M(d) = I_m - (A - BK)d$ is such that

$$\text{rank } M(\lambda) = m \quad \forall \lambda \in \bar{\mathbb{F}},$$

meaning that $\det M(d)$ must be a nonzero constant, or equivalently, that $M(d)$ is unimodular. Therefore, when we apply the feedback $u = \bar{u} - Kx$ to the system

$$\begin{cases} \sigma x = Ax + Bu \\ w = Cx + Du, \end{cases} \tag{3.22}$$

we obtain

$$\begin{cases} \sigma x = (A - BK)x + B\bar{u} \\ w = (C - DK)x + D\bar{u}. \end{cases} \tag{3.23}$$

Note that $\Sigma^{1D}(A - BK, B, C - DK, D)$ is still a minimal realization of the code, as it satisfies the conditions of Theorem 3.9. Indeed, the matrices $B$ and $D$ remain the same and hence $\begin{bmatrix} B \\ D \end{bmatrix}$ has full column rank, meaning that conditions (i) and (iii) still hold. Since controllability is not spoiled the state feedback, $(A - BK, B)$, is controllable and hence condition (ii) holds. Finally, taking $L$ and $\Lambda$ such that $B = LD$ and $\Lambda$ is a minimal left-annihilator of $D$, we have that the pair

$$(A - BK - L(C - DK), \Lambda(C - DK))$$

is given by

$$\begin{aligned} (A - BK - LC + LDK, \Lambda C - \Lambda DK) &= (A - BK - LC + BK, \Lambda C - 0K) \\ &= (A - LC, \Lambda C) \end{aligned}$$

which is an observable pair, meaning that the new realization also satisfies condition (iv) of Theorem 3.9 and is therefore minimal.

Moreover, the polynomial matrix

$$G(d) = (C - DK)(I - d(A - BK))^{-1}Bd + D$$

is polynomial and hence a (minimal) encoder of the code.

Next example illustrates the implementation of the procedure described above.

*Example* 3.14. Recalling Example 3.11 one has come to the conclusion that $\Sigma(A,B,C,D)$ is not a minimal realization of the convolutional code $\mathcal{C}$. Moreover, all conditions of Theorem 3.9 are satisfied except condition (iv), i.e. the pair $(A - LC, \Lambda C)$ is not observable. The invertible matrix $S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ reduces $\Sigma(A,B,C,D)$ to the Kalman observability decomposition, i.e., it is such that $\overline{\Sigma}(\overline{A},\overline{B},\overline{C},\overline{D}) = \overline{\Sigma}(SAS^{-1},SB,CS^{-1},D)$ has the following structure

$$\overline{A} = \begin{bmatrix} -1 & 1 & 0 \\ -1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \overline{B} = \begin{bmatrix} 1 & -1 & 1 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \overline{C} = \begin{bmatrix} 0 & -1 & 0 \end{bmatrix} \quad \text{and} \quad \overline{D} = D,$$

where the pair $\left( \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \end{bmatrix} \right)$ is observable (cf Theorem A.7 of Appendix A).

Thus, performing the coordinate change $\bar{x} = Sx$ in the state-space, and eliminating the non observable states, the equations

$$\begin{cases} \sigma x = Ax + Bu \\ w = Cx + Du, \end{cases}$$

become:

$$\begin{cases} \sigma \bar{x} = \bar{\bar{A}}\bar{x} + \bar{B}_1\bar{u}_1 \\ w = \bar{\bar{C}}\bar{x} + \bar{D}\bar{u}_1, \end{cases}$$

with

$$\bar{\bar{A}} = \begin{bmatrix} -1 & 0 \\ -1 & 0 \end{bmatrix}, \bar{B}_1 = \begin{bmatrix} 1 & -1 \\ 0 & -1 \end{bmatrix}, \bar{\bar{C}} = \begin{bmatrix} 0 & -1 \\ 0 & -1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad \bar{D} = \begin{bmatrix} 1 & -1 \\ 0 & -1 \\ 0 & -1 \end{bmatrix}.$$

This is a state-space realization for the same code as $\Sigma(A, B, C, D)$ but with smaller dimension. Moreover it can be checked that all the conditions of Theorem 3.9 are satisfied, and therefore, $\bar{\Sigma}(\bar{\bar{A}}, \bar{B}_1, \bar{\bar{C}}, \bar{D})$ is a minimal realization of the code $C$. $\diamond$

## 3.2 The two-dimensional case

When considering the realization problem of 2D convolutional codes, one can choose among different state-space models for two-dimensional processes [1, 7, 35].

In this study, we consider the Roesser model [35]. Similar to what happens with other well-known 2D state-space models, such as the Fornasini-Marchesini model [7], this model generalizes, in the two-dimensional domain, the state-space models for dynamic systems with evolution over the discrete time set (1D systems). Therefore, a state at a certain point is updated based on the state and the input values in the two nearest points in its past (the point immediately below and the point immediately on its left). However, contrary to what happens in the Fornasini-Marchesini model, in the Roesser model the state is divided into two sub-states: one which is updated in the horizontal direction and another one which is updated in the vertical direction, as we shall next see.

A very important difference between the 1D and the 2D cases has to do with the minimality of the dimension of a state-space model. Indeed, while in 1D case, minimality is characterized through properties of the model matrices, in the 2D case conditions on the matrices of a given model only allow, in general, to establish necessary or sufficient conditions for the minimality of such model [8].

### 3.2.1 The Roesser model

**Definition 3.15.** A *Roesser state-space model* is a description of a discrete time-invariant 2D system through equations of the form

$$\begin{cases} \sigma_1 x_1(i,j) = A_{11}x_1(i,j) + A_{12}x_2(i,j) + B_1 u(i,j) \\ \sigma_2 x_2(i,j) = A_{21}x_1(i,j) + A_{22}x_2(i,j) + B_2 u(i,j) \\ w(i,j) = C_1 x_1(i,j) + C_2 x_2(i,j) + Du(i,j), \end{cases} \tag{3.24}$$

where $A_{11}$, $A_{12}$, $A_{21}$, $A_{22}$, $B_1$, $B_2$, $C_1$, $C_2$ and $D$ are matrices over $\mathbb{F}$, with suitable dimensions, $\sigma_1 x_1(i,j) = x_1(i+1,j)$ and $\sigma_2 x_2(i,j) = x_2(i,j+1)$, for all $(i,j) \in \mathbb{Z}^2$, $u$ is the input-variable and $w$ is the output-variable. The variable $x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ is the state-variable, and $x_1$ and $x_2$ are the horizontal and the vertical state-variables, respectively. The sizes of the vectors $x_1$ and $x_2$ are respectively denoted by $m_1$ and $m_2$ and the size of $x$ by $m = m_1 + m_2$. The system described by (3.24) will be denoted by $\Sigma^{2D}(A_{11}, A_{12}A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$.

Note that the initial state conditions to propagate the state and output values for $i, j \geq 0$ are given by $x_1(0,j)$ for $j = 0,1,2,\ldots$ and $x_2(i,0)$ for $i = 0,1,2,\ldots$.

Next we present the solutions of (3.24) for zero initial conditions, i.e., $x_1(0,j) = 0$ and $x_2(i,0) = 0$ for $i,j = 0,1,2,\ldots$ [36]. For that purpose let us consider the state updating equation,

$$x(i,j) = A^{(1,0)}x(i-1,j) + A^{(0,1)}x(i,j-1) + B^{(1,0)}u(i-1,j) + B^{(0,1)}u(i,j-1),$$

where

$$A^{(1,0)} = \begin{bmatrix} A_{11} & A_{12} \\ 0 & 0 \end{bmatrix},\ A^{(0,1)} = \begin{bmatrix} 0 & 0 \\ A_{21} & A_{22} \end{bmatrix},\ B^{(1,0)} = \begin{bmatrix} B_1 \\ 0 \end{bmatrix} \text{ and } B^{(0,1)} = \begin{bmatrix} 0 \\ B_2 \end{bmatrix}.$$

Moreover, consider the following notations

$$\begin{aligned} A^{(i,j)} &= A^{(1,0)}A^{(i-1,j)} + A^{(0,1)}A^{(i,j-1)}, \text{ for } i,j \geq 0; \\ A^{(i,j)} &= 0, \text{ for } i < 0 \text{ or } j < 0; \quad A^{(0,0)} = I_{m_1+m_2}; \\ M(i,j) &= A^{(i-1,j)}B^{(1,0)} + A^{(i,j-1)}B^{(0,1)}, \text{ for } i,j \geq 0. \end{aligned} \tag{3.25}$$

Then, upon defining the partial order relation

$$(k,r) \leq (i,j) \Leftrightarrow k \leq i \wedge r \leq j,$$

for zero initial conditions and an input sequence $u(\cdot,\cdot)$ defined in the positive quadrant of $\mathbb{Z}^2$, the state and the output sequences are given by

$$x(i,j) = \sum_{\substack{0<s\leq i \\ 0<r\leq j}} M(s,r)u(i-s,j-r)$$

and

$$w(i,j) = \sum_{\substack{0<s\leq i \\ 0<r\leq j}} CM(s,r)u(i-s,j-r) + Du(i,j), \tag{3.26}$$

where $C = \begin{bmatrix} C_1 & C_2 \end{bmatrix}$.

The following notions, defined as in [35] and [21], are fundamental to establish a necessary and sufficient condition for the minimality of a specific class of 2D Roesser models.

**Definition 3.16.** The 2D state-space model (3.24) is said to be:

1. *locally controllable* if, upon assuming zero initial conditions for the state, and given an arbitrary state vector $x^*$ of $\mathbb{F}^{m_1+m_2}$, there exist integers $N,Q > 0$, and an input sequence $u(\cdot,\cdot)$ such that $x(N,Q) = x^*$;

2. *locally unobservable* if there exists a nonzero initial state, $x(0,0)$, such that when the remaining state initial conditions $x_1(0,j)$, $x_2(i,0)$ are zero for $i > 0$ and $j > 0$ and the input is zero, i.e., $u(\cdot,\cdot) \equiv 0$, then $w(\cdot,\cdot) \equiv 0$.

Defining the controllability and observability matrices as

$$\begin{aligned} C_{m_1,m_2} \;=\; & \Big[\; M(1,0) \quad M(2,0) \quad \dots \quad M(m_1,0) \;\Big| \\ & \quad M(0,1) \quad M(1,1) \quad \cdots \quad M(m_1,1) \\ & \Big|\dots\Big|\; M(0,m_2) \quad M(1,m_2) \quad \dots \quad M(m_1,m_2) \;\Big] \end{aligned} \tag{3.27}$$

and

$$\begin{aligned} \mathcal{O}_{m_1,m_2} = \Big[ & (CA^{(0,0)})^T \quad (CA^{(0,1)})^T \quad \dots \quad (CA^{(0,m_2)})^T \Big| \\ & \Big| \dots \Big| \ (CA^{(m_1-1,0)})^T \quad (CA^{(m_1-1,1)})^T \quad \dots \quad (CA^{(m_1-1,m_2)})^T \Big| \\ & (CA^{(m_1,0)})^T \quad (CA^{(m_1,1)})^T \quad \dots \quad (CA^{(m_1,m_2-1)})^T \Big]^T, \end{aligned} \tag{3.28}$$

respectively, we can state the following characterization of controllability and observability for a 2D Roesser state-space model.

**Proposition 3.17.** *[21, 35] The 2D state-space model* (3.24) *is:*

1. *locally controllable if and only if* $\operatorname{rank} \mathcal{C}_{m_1,m_2} = m_1 + m_2$*;*
2. *locally observable if and only if* $\operatorname{rank} \mathcal{O}_{m_1,m_2} = m_1 + m_2$.

The partition of the state in its horizontal and vertical components motivates the partition of the controllability and observability matrices as follows [35].

$$\mathcal{C}_{m_1,m_2} = \left[\begin{array}{c} \mathcal{C}^h_{m_1,m_2} \\ \hline \mathcal{C}^v_{m_1,m_2} \end{array}\right] \text{ and } \mathcal{O}_{m_1,m_2} = \left[\begin{array}{c|c} \mathcal{O}^h_{m_1,m_2} & \mathcal{O}^v_{m_1,m_2} \end{array}\right], \tag{3.29}$$

where

$$\begin{aligned} &\mathcal{C}^h_{m_1,m_2} \in \mathbb{R}^{m_1 \times \left[\left((m_1+1)(m_2+1)-1\right)k\right]}, \quad \mathcal{O}^h_{m_1,m_2} \in \mathbb{R}^{\left[\left((m_1+1)(m_2+1)-1\right)n\right] \times m_1}, \\ &\mathcal{C}^v_{m_1,m_2} \in \mathbb{R}^{m_2 \times \left[\left((m_1+1)(m_2+1)-1\right)k\right]} \text{ and } \mathcal{O}^v_{m_1,m_2} \in \mathbb{R}^{\left[\left((m_1+1)(m_2+1)-1\right)n\right] \times m_2} \end{aligned}$$

denote the controllability and observability matrices associated with vertical and horizontal components, respectively. The sets $X^c_h = \operatorname{Im} \mathcal{C}^h_{m_1,m_2} \subseteq \mathbb{F}^m_1$, $X^c_v = \operatorname{Im} \mathcal{C}^v_{m_1,m_2} \subseteq \mathbb{F}^m_2$, $X^u_h = \ker \mathcal{O}^h_{m_1,m_2} \subseteq \mathbb{F}^m_1$ and $X^u_v = \ker \mathcal{O}^v_{m_1,m_2} \subseteq \mathbb{F}^m_2$ are called *horizontal controllable* state-space, *vertical controllable* state-space, *horizontal unobservable* state-space and *vertical unobservable* state-space, respectively.

### 3.2.2 The separable Roesser model

In the sequel we consider a special type of Roesser models known as the *separable Roesser models*. In these models the state updating in one of two directions can be done

separately from the other direction [35]. Thus, the dynamics along the direction with separate updating coincides with a one-dimensional dynamics.

More concretely, such models are characterized by one of the matrices $A_{12}$ or $A_{21}$ in (3.24) being zero. From now on we shall consider Roesser models with $A_{12} = 0$ (the study for $A_{21} = 0$ is similar), i.e., models described through equations of the form:

$$\begin{cases} \sigma_1 x_1(i,j) = A_{11}x_1(i,j) + B_1 u(i,j) \\ \sigma_2 x_2(i,j) = A_{21}x_1(i,j) + A_{22}x_2(i,j) + B_2 u(i,j) \\ w(i,j) = C_1 x_1(i,j) + C_2 x_2(i,j) + Du(i,j), \end{cases} \tag{3.30}$$

where the notation is the same as in (3.24). For simplicity we denote equations (3.30) by $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$.

As we shall latter see in Theorem 3.26, 2D separable Roesser models are particularly nice since they admit a necessary and sufficient condition for minimality that can easily be expressed in terms of the matrices of the system. Such conditions are stated in terms of special local controllability and observability properties.

In order to study local controllability and observability properties for the separable case note that, in this case, the following relations hold from (3.25), see [17].

$$\begin{aligned} A^{(i,0)} &= \{A^{(1,0)}\}^i = \left[\begin{array}{c|c} A_{11}^i & 0 \\ \hline 0 & 0 \end{array}\right]; \\ A^{(0,j)} &= \{A^{(0,1)}\}^j = \left[\begin{array}{c|c} 0 & 0 \\ \hline A_{22}^{j-1}A_{21} & A_{22}^j \end{array}\right]; \\ A^{(i,j)} &= \left[\begin{array}{c|c} 0 & 0 \\ \hline A_{22}^{j-1}A_{21}A_{11}^i & 0 \end{array}\right], \text{ for } i,j \geq 1; \end{aligned} \tag{3.31}$$

and

$$\begin{aligned} M(i,0) &= \left[\begin{array}{c} A_{11}^{i-1}B_1 \\ \hline 0 \end{array}\right]; \; M(0,j) = \left[\begin{array}{c} 0 \\ \hline A_{22}^{j-1}B_2 \end{array}\right]; \\ M(i,j) &= \left[\begin{array}{c} 0 \\ \hline A_{22}^{j-1}A_{21}A_{11}^{i-1}B_1 \end{array}\right], \text{ for } i,j \geq 1. \end{aligned} \tag{3.32}$$

Thus, for separable systems we obtain a specific structure for the controllability and observability matrices as follows

$$\mathcal{C}_{m_1,m_2} = \left[\begin{array}{c|c} P_{m_1} & 0 \\ \hline 0 & \mathcal{P}_{m_1,m_2} \end{array}\right], \quad \mathcal{O}_{m_1,m_2} = \left[\begin{array}{c|c} \mathcal{L}_{m_1,m_2} & Q_{m_2+1} \\ \overline{C}_{m_2-1}A_{11}^{m_1} & 0 \end{array}\right], \tag{3.33}$$

where, for $i, j \geq 1$,

$$P_i = \left[\begin{array}{c|c|c|c} B_1 & A_{11}B_1 & \cdots & A_{11}^{i-1}B_1 \end{array}\right] \in \mathbb{F}^{m_1 \times ki}, \tag{3.34}$$

$$\mathcal{P}_{i,j} = \left[\begin{array}{c|c|c|c} \overline{B}_i & A_{22}\overline{B}_i & \cdots & A_{22}^{j-1}\overline{B}_i \end{array}\right] \in \mathbb{F}^{m_2 \times jk(i+1)}, \tag{3.35}$$

with $\overline{B}_i = \left[\begin{array}{c|c} B_2 & A_{21}P_i \end{array}\right] \in \mathbb{F}^{m_2 \times k(i+1)}$ and

$$Q_j = \left[(C_2)^T \quad \cdots \quad (C_2A_{22}^{j-1})^T\right]^T \in \mathbb{F}^{nj \times m_2}, \tag{3.36}$$

$$\mathcal{L}_{i,j} = \left[(\overline{C}_j)^T \quad \cdots \quad (\overline{C}_jA_{11}^{i-1})^T\right]^T \in \mathbb{F}^{in(j+1) \times m_1}, \tag{3.37}$$

with $\overline{C}_j = \left[C_1^T \quad (Q_jA_{21})^T\right]^T \in \mathbb{F}^{n(j+1)\times m_1}$.

Since rank $\mathcal{C}_{m_1,m_2}^h$ = rank $P_{m_1}$ and rank $\mathcal{C}_{m_1,m_2}^v$ = rank $\mathcal{P}_{m_1,m_2}$, we will call suggestively $P_{m_1}$ and $\mathcal{P}_{m_1,m_2}$ by *horizontal controllability matrix* and *vertical controllability matrix*, respectively. Similarly, since rank $\mathcal{O}_{m_1,m_2}^h$ = rank $\mathcal{L}_{m_1,m_2}$ and rank $\mathcal{O}_{m_1,m_2}^v$ = rank $Q_{m_2}$, we will call $\mathcal{L}_{m_1,m_2}$ and $Q_{m_2}$ by *horizontal observability matrix* and *vertical observability matrix*, respectively.

In the separable case, we define separable controllability and separable observability as follows.

**Definition 3.18.** A 2D separable Roesser model is said to be:

1. *separately locally controllable* if $X_h^c = \mathbb{F}^{m_1}$ and $X_v^c = \mathbb{F}^{m_2}$;

2. *separately locally unobservable* if $X_h^u = \{0_{m_1}\}$ and $X_v^u = \{0_{m_2}\}$.

These properties can be characterized in terms of the matrices previously defined by means of the next proposition.

**Proposition 3.19.** *[21] The 2D state-space model* (3.24) *is:*

1. *separately locally controllable if and only if* $\operatorname{rank} C^h_{m_1,m_2} = m_1$ *and* $\operatorname{rank} C^v_{m_1,m_2} = m_2$.
2. *separately locally observable if and only if* $\operatorname{rank} O^h_{m_1,m_2} = m_1$ *and* $\operatorname{rank} O^v_{m_1,m_2} = m_2$.

From (3.33) it follows that a separable system is separately locally controllable if and only if it is locally controllable. The same cannot be concluded for the observability. In fact, local observability implies separable local observability but the opposite is not true [17].

*Example* 3.20. Let us consider $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$, where $A_{11} = A_{21} = A_{22} = D = 0$ and $B_1 = B_2 = C_1 = C_2 = 1$ corresponding the following equations:

$$\begin{cases} x^h(i+1,j) = u(i,j) \\ x^v(i,j+1) = u(i,j) \\ y(i,j) = x^h(i,j) + x^v(i,j), \end{cases} \tag{3.38}$$

Taking into account the observability matrix of the system, given by

$$O_{1,1} = \begin{bmatrix} 1 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix},$$

we have that $\operatorname{rank} O_{1,1} = 1 \neq 2 = 1 + 1 = m_1 + m_2$. Thus, by Proposition 3.17 we conclude that $\Sigma^{2D}$ is not locally observable.

However, partitioning the observability matrix in it horizontal and vertical components we have that

$$\operatorname{rank} O^h_{1,1} = \operatorname{rank} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = 1 \quad \text{and} \quad \operatorname{rank} O^v_{1,1} = \operatorname{rank} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = 1.$$

Consequently, by Proposition 3.19, $\Sigma^{2D}$ is separately locally observable. ◇

### 3.2.3 Realizations of 2D encoders via separable Roesser models

**Definition 3.21.** $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$ is said to be a *realization* of an encoder $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$ if

$$G(d_1, d_2) = \bar{C}\bar{A}(d_1, d_2)^{-1}\bar{B}(d_1, d_2) + D,$$

where

$$\bar{C} = \begin{bmatrix} C_1 & C_2 \end{bmatrix}, \quad \bar{A}(d_1, d_2) = \begin{bmatrix} I_{m_1} - A_{11}d_1 & 0 \\ -A_{21}d_2 & I_{m_2} - A_{22}d_2 \end{bmatrix}$$

and

$$\bar{B}(d_1, d_2) = \begin{bmatrix} B_1 \\ 0 \end{bmatrix} d_1 + \begin{bmatrix} 0 \\ B_2 \end{bmatrix} d_2.$$

Similarly to what happens in the 1D case, under the light of the behavioral approach, this is equivalent to say that $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$ is a realization of an encoder $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$ if the behavior

$$\mathcal{B}_{(u,w)} = \{(u, w) \mid \hat{w}(d_1, d_2) = G(d_1, d_2)\hat{u}(d_1, d_2)\}$$

coincides with the set

$$\{(u, w) \mid \exists\ x = (x_1, x_2) \text{ such that } (u, x, w) \text{ satisfies(3.30)}\}.$$

In the sequel, this fact is expressed by the equality

$$\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D) = \Sigma^{2D}(G).$$

In [34] it was shown (although in a different context) that every $2D$ encoder $G(d_1, d_2)$ can be realized by a 2D separable Roesser model.

**Definition 3.22.** $\Sigma^{2D}(G)$ is said to be a *minimal realization* of $G(d_1, d_2)$ if the size of the state $x = (x_1, x_2)$ is minimal among all the realizations of $G(d_1, d_2)$. Moreover, given a polynomial matrix $G(d_1, d_2)$ we define the *Roesser McMillan degree* of $G(d_1, d_2)$, $\mu_R(G)$, as the minimal dimension of a realization as in (3.30) of $G(d_1, d_2)$.

Note that different polynomial encoders of a 2D convolutional code may have different Roesser McMillan degrees.

The next theorem provides a procedure for obtaining a minimal realization for an arbitrary polynomial matrix $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$.

**Theorem 3.23.** *[17] Let $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$. Write*

$$G(d_1, d_2) = G_2(d_2)G_1(d_1), \tag{3.39}$$

*with*

$$G_2(d_2) = \left[ I_n \mid I_n d_2 \mid \cdots \mid I_n d_2^{\ell_2} \right] N_2, \tag{3.40}$$

*where $N_2$ is a full column rank constant matrix and $\ell_2$ is the highest exponent of $d_2$ appearing in $G(d_1, d_2)$ and*

$$G_1(d_1) = N_1 \begin{bmatrix} I_k \\ I_k d_1 \\ \vdots \\ I_k d_1^{\ell_1} \end{bmatrix}, \tag{3.41}$$

*where $N_1$ is a full row rank constant matrix and $\ell_1$ is the highest exponent of $d_1$ appearing in $G(d_1, d_2)$.*

*Let $\Sigma^{1D}(A_{11}, B_1, \bar{C}_1, \bar{D}_1)$ and $\Sigma^{1D}(A_{22}, \bar{B}_2, C_2, \bar{D}_2)$ be 1D minimal realizations of $G_1(d_1)$ and $G_2(d_2)$ of dimensions $m_1$ and $m_2$, respectively. Then $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$, where $A_{21} = \bar{B}_2\bar{C}_1$, $B_2 = \bar{B}_2\bar{D}_1$, $C_1 = \bar{D}_2\bar{C}_1$ and $D = \bar{D}_2\bar{D}_1$ is a 2D minimal realization of $G(d_1, d_2)$ of dimension $m = m_1 + m_2$.*

*Example* 3.24. Consider the right-factor prime encoder

$$G(d_1,d_2) = \begin{bmatrix} 1+d_1^2+d_1d_2+d_2d_1^2 \\ 1+2d_1+3d_1^2+2d_1^2d_2+d_1d_2+d_2 \end{bmatrix}$$
$$= \begin{bmatrix} 1 & 0 & d_2 & 0 \\ 0 & 1 & 0 & d_2 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ d_1 \\ d_1^2 \end{bmatrix}.$$

Note that $\begin{bmatrix} 1 & 0 & 1 \\ 1 & 2 & 3 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$, with $N_2 = \begin{bmatrix} 1 & 0 \\ 1 & 2 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}$ full column rank and $N_1 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ full row rank.

Let us now consider $G(d_1,d_2)$ factorized as $G(d_1,d_2) = G_2(d_2)G_1(d_1)$, with

$$G_2(d_2) = \begin{bmatrix} 1 & 0 & d_2 & 0 \\ 0 & 1 & 0 & d_2 \end{bmatrix} N_2 \text{ and } G_1(d_1) = N_1 \begin{bmatrix} 1 \\ d_1 \\ d_1^2 \end{bmatrix}$$

. Then, $\Sigma^{1D}(A_{22},\bar{B}_2,C_2,\bar{D}_2)$, where

$$A_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad \bar{B}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } \bar{D}_2 = \begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$$

and $\Sigma^{1D}(A_{11},B_1,\bar{C}_1,\bar{D}_1)$, where

$$A_{11} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \bar{C}_1 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } \bar{D}_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

are minimal 1D realizations of

$$G_2(d_2) = \begin{bmatrix} 1 & d_2 \\ 1+d_2 & 2+d_2 \end{bmatrix} \quad \text{and} \quad G_1(d_1) = \begin{bmatrix} 1+d_1^2 \\ d_1+d_1^2 \end{bmatrix},$$

respectively, both with dimension 2. Thus $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$, where

$$A_{11} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad A_{21} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad A_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad B_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$C_1 = \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \text{ and } D = \begin{bmatrix} 1 \\ 1 \end{bmatrix},$$

obtained by applying Theorem 3.23, is a minimal realization of $G(d_1, d_2)$, of dimension 4. ◇

**Remark 3.25.** *Note that the factorization presented in (3.39), (3.40) and (3.41) in the above theorem, can be easily determined by writing*

$$G(d_1, d_2) = \left[ I_n \;\middle|\; I_n d_2 \;\middle|\; \cdots \;\middle|\; I_n d_2^{\ell_2} \right] N \begin{bmatrix} I_k \\ I_k d_1 \\ \vdots \\ I_k d_1^{\ell_1} \end{bmatrix}, \tag{3.42}$$

*where $N$ is a constant matrix. If $N$ has rank $p$, there exists a full column rank constant matrix $N_2$ with $p$ columns, and a full row rank constant matrix $N_1$ with $p$ rows such that $N = N_2 N_1$. Note that the decomposition (3.42) is not unique. Nevertheless, there exists a relation between all the possible factorizations. For instance, suppose now that $G(d_1, d_2)$ can also be factorized in another way, let is say*

$$G(d_1, d_2) = \bar{G}_2(d_2)\bar{G}_1(d_1), \tag{3.43}$$

*with*

$$\bar{G}_2(d_2) = \left[ I_n \;\middle|\; I_n d_2 \;\middle|\; \cdots \;\middle|\; I_n d_1^{\ell_2} \right] \bar{N}_2, \tag{3.44}$$

*where $\bar{N}_2$ is a full column rank constant matrix, with rank $r \leq p$, and*

$$\bar{G}_1(d_1) = \bar{N}_1 \begin{bmatrix} I_k \\ I_k d_1 \\ \vdots \\ I_k d_2^{\ell_1} \end{bmatrix}, \tag{3.45}$$

*where $\bar{N}_1$ is a full row rank constant matrix, with rank $r$. Then,*

$$N_2 N_1 = \bar{N}_2 \bar{N}_1. \tag{3.46}$$

*Since $N_2$ and $N_1$ are full column and full row rank, respectively, they admit left and right inverses, say $M_2$ and $M_1$, respectively. Thus, (3.46) yields*

$$N_1 = T\bar{N}_1, \tag{3.47}$$

*where $T = M_2\bar{N}_2$ is an invertible matrix of adequate size. Replacing (3.47) in (3.46), we get*

$$N_2 = T^{-1}\bar{N}_2. \tag{3.48}$$

*From (3.47) and (3.48) we can conclude that there exists a unique factorization of $G(d_1, d_2)$ of the form (3.39) up to a constant invertible matrix $T$. Consequently, if $\Sigma^{1D}(A_2, B_2, C_2, D_2)$ and $\Sigma^{1D}(A_1, B_1, C_1, D_1)$ are realizations of $G_2(d_2)$ and $G_1(d_1)$, respectively, then $\bar{G}_2(d_2)$ and $\bar{G}_1(d_1)$ are realized by $\bar{\Sigma}^{1D}(A_2, B_2T, C_2, D_2T)$ and $\bar{\Sigma}^{1D}(A_1, B_1, T^{-1}C_1, T^{-1}D_1)$, respectively.*

Concerning the separable Roesser model, in [17], a necessary and sufficient condition for minimality was presented, as stated in the next result using the language of codes.

**Theorem 3.26.** *[17] Let $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$ be an encoder of a convolutional code $C$. Then $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$ is a minimal realization of the encoder $G(d_1, d_2)$ if and only if is separately locally controllable and separately locally observable.*

**Remark 3.27.** *Note that a polynomial matrix $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$ can also be factorized as $\bar{G}_1(d_1)\bar{G}_2(d_2)$, for some polynomial matrices $\bar{G}_2(d_2)$ and $\bar{G}_1(d_1)$ of suitable sizes. However, here we have considered the factorization $G(d_1, d_2) = G_2(d_2)G_1(d_1)$, since this is the one that corresponds to the form that we have considered for the separable Roesser model (with $A_{12} = 0$).*

### 3.2.4 Realizations of 2D convolutional codes via separable Roesser models

**Definition 3.28.** $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$ is said to be a *(separable Roesser model) realization* of the 2D convolutional code $\mathcal{C}$ if the corresponding $w$–behavior

$$\mathcal{B}_w = \{w \mid \mathbb{Z}^2 \to \mathbb{F}^n : \exists\, x_1, x_2, u \text{ such that } (u, x_1, x_2, w) \text{ satisfies (3.30)}\}$$

coincides with $\mathcal{C}$, that is, $\mathcal{B}_w = \mathcal{C}$.

This is denoted by $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D) = \Sigma^{2D}(\mathcal{C})$.

From now on separable Roesser model realizations will be simply referred as "realizations".

**Definition 3.29.** $\Sigma^{2D}(\mathcal{C})$ is said to be a *minimal realization* of the 2D code $\mathcal{C}$ if the size of $(x_1, x_2, u)$ is minimal among all the realizations of $\mathcal{C}$. Moreover, we define the *Roesser McMillan degree of* $\mathcal{C}$, $\mu_R^*(\mathcal{C})$, as the minimum of the Roesser McMillan degrees of all polynomial encoders of $\mathcal{C}$. The polynomial encoders $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n \times k}$ with Roesser McMillan degree $\mu_R(G)$ such that

$$\mu_R^*(\mathcal{C}) = \mu_R(G) + k$$

are called *Roesser minimal* ($R$-minimal) encoders of $\mathcal{C}$.

Contrary to what happens in the 1D case, it seems hard to obtain necessary and sufficient conditions for the minimality of realizations of a 2D convolutional code.

As shown in [34], every 2D convolutional code can be realized by means of a model of the type (3.30) taking advantage of the factorization given in Theorem 3.23. However, it still seems hard to obtain necessary and sufficient conditions for the minimality of the 2D realizations.

We next present the part of the result obtained in [34] concerning the sufficient conditions for minimality of separable Roesser models realizations of 2D codes, and redo its proof with more detail since it was originally presented only in a very succinct way.

**Proposition 3.30.** *Let $C$ be a 2D convolutional code and let*

$$\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D) = \Sigma^{2D}(C)$$

*be a realization of $C$. Denote*

$$\Sigma_1^{1D} = \Sigma^{1D}\left(A_{11}, B_1, \begin{bmatrix} A_{21} \\ C_1 \end{bmatrix}, \begin{bmatrix} B_2 \\ D \end{bmatrix}\right)$$

*and*

$$\Sigma_2^{1D} = \Sigma^{1D}\left(A_{22}, \begin{bmatrix} A_{21} & B_2 \end{bmatrix}, C_2, \begin{bmatrix} C_1 & D \end{bmatrix}\right)$$

*and suppose that $\Sigma_1^{1D}$ and $\Sigma_2^{1D}$ are both minimal realizations of the corresponding output behaviors. Then $\Sigma^{2D}(C)$ is a minimal realization for $C$.*

*Proof.* We first prove that $\Sigma_2^{1D}$ is a (minimal) realization of the 1D code

$$C\,|_{\mathcal{L}_i} = \{\bar{w} \mid \exists\, w \in C \text{ such that } w\,|_{\mathcal{L}_i} = \bar{w}\}$$

, where $\mathcal{L}_i = \{(i, j), j \in \mathbb{Z}\}$, for $i \in \mathbb{Z}$. For this purpose we have to show that the output behavior of $\Sigma_2^{1D}$ coincides with $C\,|_{\mathcal{L}_i}$. We only prove the result for $i = 0$. Due to shift-invariance, the result also holds for other $i$'s.

i) Firstly suppose that $(\bar{w}, \bar{x}_1, \bar{x}_2, \bar{u})$ satisfy the following equations:

$$\begin{cases} \sigma\bar{x}_2 = A_{22}\bar{x}_2 + \begin{bmatrix} A_{21} & B_2 \end{bmatrix} \begin{bmatrix} \bar{x}_1 \\ \bar{u} \end{bmatrix} \\ \bar{w} = C_2\bar{x}_2 + \begin{bmatrix} C_1 & D \end{bmatrix} \begin{bmatrix} \bar{x}_1 \\ \bar{u} \end{bmatrix}, \end{cases} \tag{3.49}$$

In order to prove that $\bar{w} \in C|_{\mathcal{L}_0}$ we shall construct a 2D trajectory, $(w, x_2, (x_1, u))$, which satisfies the equations of $\Sigma^{2D}(C)$ and such that $w(0, \cdot) = \bar{w}(\cdot)$.

Define $\bar{x}_1^{(1)} = A_{11}\bar{x}_1 + B_1\bar{u}$. Take an arbitrary $\bar{u}^{(1)}$ and define $\bar{x}_2^{(1)}$ such that

$$\sigma\bar{x}_2^{(1)} = A_{22}\bar{x}_2^{(1)} + \begin{bmatrix} A_{21} & B_2 \end{bmatrix} \begin{bmatrix} \bar{x}_1^{(1)} \\ \bar{u}^{(1)} \end{bmatrix} \text{ and } \bar{w}^{(1)} = C_2\bar{x}_2^{(1)} + \begin{bmatrix} C_1 & D \end{bmatrix} \begin{bmatrix} \bar{x}_1^{(1)} \\ \bar{u}^{(1)} \end{bmatrix}.$$

Define also

$$w(0,\cdot) = \bar{w},\ x_2(0,\cdot) = \bar{x}_2,\ x_1(0,\cdot) = \bar{x}_1,\ u(0,\cdot) = \bar{u}$$

and

$$w(1,\cdot) = \bar{w}^{(1)},\ x_2(1,\cdot) = \bar{x}_2^{(1)},\ x_1(1,\cdot) = \bar{x}_1^{(1)},\ u(1,\cdot) = \bar{u}^{(1)}.$$

Consider now $\bar{x}_1^{(-1)}$ and $\bar{u}^{(-1)}$ such that $\bar{x}_1 = A_{11}\bar{x}_1^{(-1)} + B_1\bar{u}^{(-1)}$. Note that, since $\Sigma_1^{1D}$ is a minimal 1D code realization, $\begin{bmatrix} A_{11} & B_1 \end{bmatrix}$ has full row rank (because $(A_{11}, B_1)$ is controllable) and therefore there exist such $\bar{x}_1^{(-1)}$ and $\bar{u}^{(-1)}$.

Define $\bar{x}_2^{(-1)}$ such that

$$\begin{cases} \sigma\bar{x}_2^{(-1)} = A_{22}\bar{x}_2^{(-1)} + \begin{bmatrix} A_{21} & B_2 \end{bmatrix} \begin{bmatrix} \bar{x}_1^{(-1)} \\ \bar{u}^{(-1)} \end{bmatrix} \\ \bar{w}^{(-1)} = C_2\bar{x}_2^{(-1)} + \begin{bmatrix} C_1 & D \end{bmatrix} \begin{bmatrix} \bar{x}_1^{(-1)} \\ \bar{u}^{(-1)} \end{bmatrix}, \end{cases}$$

and

$$w(-1,\cdot) = \bar{w}^{(-1)},\ x_2(-1,\cdot) = \bar{x}_2^{(-1)},\ x_1(-1,\cdot) = \bar{x}_1^{(-1)},\ u(-1,\cdot) = \bar{u}^{(-1)}$$

Continuing in this way we define a trajectory $(w, x_1, x_2, u)$ which satisfies the equations of $\Sigma^{2D}(C)$ and such that $w(0,\cdot) = \bar{w}(\cdot)$. Since, by assumption, $\Sigma^{2D}(C)$ is a realization of $C$, $w \in C$. Moreover, since $w(0,\cdot) = \bar{w}(\cdot)$, this implies that $\bar{w} \in C|_{\mathcal{L}_0}$. Consequently the output behavior of $\Sigma_2^{1D}$ is contained in $C|_{\mathcal{L}_0}$.

ii) In order to prove that $C|_{\mathcal{L}_0}$ is contained in the output behavior of $\Sigma_2^{1D}$, take $\bar{w} \in C|_{\mathcal{L}_0}$. Then there exists $w \in C$ such that $\bar{w}(\cdot) = w(0,\cdot)$. Since $\Sigma^{2D}(C)$ is a (separable) realization of $C$ there exists $x_2$, $x_1$ and $u$ such that

$$\begin{cases} \sigma_1 x_1 = A_{11}x_1 + B_1 u \\ \sigma_2 x_2 = A_{21}x_1 + A_{22}x_2 + B_2 u \\ w = C_1 x_1 + C_2 x_2 + Du. \end{cases}$$

Consequently,

$$\begin{cases} x_2(0, j+1) = A_{21}x_1(0, j) + A_{22}x_2(0, j) + B_2u(0, j) \\ w(0, j) = C_1x_1(0, j) + C_2x_2(0, j) + Du(0, j), \end{cases}$$

where $w(0, j) = \bar{w}(j)$.

Therefore, defining $\bar{x}_2(\cdot) = x_2(0, \cdot)$, $\bar{x}_1(\cdot) = x_1(0, \cdot)$ and $\bar{u}(\cdot) = u(0, \cdot)$, we obtain

$$\begin{cases} \bar{x}_2(j+1) = A_{21}\bar{x}_1(j) + A_{22}\bar{x}_2(j) + B_2\bar{u}(j) \\ \bar{w}(j) = C_1\bar{x}_1(j) + C_2\bar{x}_2(j) + D\bar{u}(j). \end{cases}$$

Hence, $C|_{\mathcal{L}_0}$ is contained in the output behavior of $\Sigma_2^{1D}$.

From i) and ii) we conclude that $\Sigma_2^{1D}$ is a (minimal) realization of the 1D code $C|_{\mathcal{L}_0}$.

Now, this means that the sizes of the variables $\bar{x}_1$, $\bar{x}_2$ and $\bar{u}$ cannot be decreased in $\Sigma_2^{1D}$, which implies that the size of $x_1$, $x_2$ and $u$ cannot be decreased in $\Sigma^{2D}(C)$ if one wishes that this is a realization of $C$. Consequently, the assumptions of the proposition imply that $\Sigma^{2D}(C)$ is a minimal (separable Roesser model) realization of the code $C$. □

The result of Proposition 3.30 will be useful for the minimal realization of composition codes, to be considered in Chapter 5 of this thesis.

# Chapter 4

# Minimal realizations of 2D convolutional codes

As shown in section 3.1.2.1, it is possible to obtain a minimal realization of a 1D code $\mathcal{C}$ by eliminating superfluous variables from a minimal realization of an encoder $G(d)$ of $\mathcal{C}$. However, an alternative approach has been considered in [9, 11, 12] that consists in first selecting a minimal encoder $G^*(d)$ of $\mathcal{C}$ and then performing a minimal realization of that encoder $G^*(d)$. This presupposes a characterization of minimal encoders. Such characterization has been given in [9, 11, 12]. In particular, it turns out that 1D canonical (i.e., right-prime and reduced) encoders are among the minimal ones.

In this chapter we make an attempt to obtain similar results regarding the characterization of minimal 2D encoders having in mind the construction of minimal code realizations.

We start by considering the class of 2D convolutional codes of rate $1/n$. Then some considerations about the difficulties on the generalization of the obtained results to convolutional codes of rate $k/n$, for $k > 1$ are presented.

## 4.1 Minimal 2D realizations of 2D convolutional codes of rate $1/n$

In this section we restrict our study to two-dimensional convolutional codes with rate $1/n$ and investigate the problem of obtaining minimal realizations of such codes by separable Roesser models. For this purpose we first characterize the minimal encoders with respect to this type of model (i.e., the $R$-minimal encoders).

The 2D convolutional codes with rate $1/n$ are the ones which admit encoders of size $n \times 1$. In the 1D case, the minimal encoders of a convolutional code of rate $1/n$ are the right-prime encoders [9]. The next result proves that this also holds in the 2D case for $R$-minimal encoders.

**Theorem 4.1.** *Let $C$ be a 2D convolutional code of rate $1/n$. Then the $R$-minimal encoders of $C$ are the right-factor prime encoders of $C$.*

*Proof.* Let $C$ be a 2D convolutional code of rate $\frac{1}{n}$, i.e., that admits encoders of size $n \times 1$. Let us consider two equivalent polynomial encoders of $C$, $G(d_1, d_2)$ and $\tilde{G}(d_1, d_2)$ (of size $n \times 1$). According to the properties of equivalent encoders, observe that if $G(d_1, d_2)$ and $\tilde{G}(d_1, d_2)$ are both right-factor prime encoders, then they differ by a nonzero constant and thus minimal 2D realizations as in (3.30) of $G(d_1, d_2)$ and $\tilde{G}(d_1, d_2)$ have the same dimension.

Let us consider now that $\bar{G}(d_1, d_2)$ is an equivalent encoder of $G(d_1, d_2)$ such that

$$\bar{G}(d_1, d_2) = G(d_1, d_2)p(d_1, d_2), \tag{4.1}$$

for some polynomial $p(d_1, d_2) \in \mathbb{F}[d_1, d_2]$ and let us see that the Roesser McMillan degree of $\bar{G}(d_1, d_2)$ is equal to or greater than the Roesser McMillan degree of $G(d_1, d_2)$, i.e.,

$$\mu_R(\bar{G}) \geq \mu_R(G).$$

The polynomial $p(d_1, d_2)$ can be regarded as a polynomial in $d_1$ with coefficients over $\mathbb{F}[d_2]$, i.e., for some $\nu_1 \in \mathbb{N}$

$$p(d_1, d_2) = p_0(d_2) + p_1(d_2)d_1 + \cdots + p_{\nu_1}(d_2)d_1^{\nu_1}, \tag{4.2}$$

where $p_i(d_2) \in \mathbb{F}[d_2]$, for $i = 0, \cdots, \nu_1$, with $p_{\nu_1}(d_2) \neq 0$.

Let $G(d_1, d_2)$ be factorized as

$$G(d_1, d_2) = G_2(d_2)G_1(d_1),$$

with

$$G_2(d_2) = \left[ I_n \;\middle|\; I_n d_2 \;\middle|\; \cdots \;\middle|\; I_n d_2^{\ell_2} \right] N,$$

where $N$ is a constant matrix and

$$G_1(d_1) = \begin{bmatrix} 1 & \cdots & d_1^{\ell_1} \end{bmatrix}^T,$$

for some $\ell_1, \ell_2 \in \mathbb{N}$ as in Theorem 3.23. Let us consider two cases:

**Case 1** $N$ is full column rank

Write $G_2(d_2) = \begin{bmatrix} C_0(d_2) & C_1(d_2) & \cdots & C_{\ell_1}(d_2) \end{bmatrix}$, where $C_i(d_2) \in \mathbb{F}[d_2]^n$ are the columns of $G_2(d_2)$, for $i = 0, \ldots, \ell_1$. Then

$$\begin{aligned} G(d_1, d_2)p(d_1, d_2) &= \begin{bmatrix} C_0(d_2) & C_1(d_2) & \cdots & C_{\ell_1}(d_2) \end{bmatrix} \begin{bmatrix} 1 \\ \vdots \\ d_1^{\ell_1} \end{bmatrix} p(d_1, d_2) \\ &= \begin{bmatrix} C_0(d_2) & C_1(d_2) & \cdots & C_{\ell_1}(d_2) \end{bmatrix} P(d_2) \begin{bmatrix} 1 \\ d_1 \\ \vdots \\ d_1^{\ell_1+\nu_1} \end{bmatrix}, \end{aligned}$$

where

$$P(d_2) = \begin{bmatrix} p_0(d_2) & p_1(d_2) & & & p_{\nu_1}(d_2) & & & 0 \\ & p_0(d_2) & p_1(d_2) & & & p_{\nu_1}(d_2) & & \\ & & \ddots & \ddots & & & \ddots & \\ 0 & & & p_0(d_2) & p_1(d_2) & & & p_{\nu_1}(d_2) \end{bmatrix}$$

has dimension $(\ell_1+1)\times(\ell_1+\nu_1+1)$. Therefore $\bar{G}(d_1,d_2)$ can be factorized as follows

$$G(d_1,d_2)p(d_1,d_2)=\bar{G}_2(d_2)\bar{G}_1(d_1),$$

where

$$\bar{G}_2(d_2)=\begin{bmatrix}C_0(d_2) & \cdots & C_{\ell_1}(d_2)\end{bmatrix}P(d_2)$$

and

$$\bar{G}_1(d_1)=\left[\begin{array}{c|c|c|c}1 & d_1 & \cdots & d_1^{\ell_1+\nu_1}\end{array}\right]^T,$$

Let us see now that there exists a minor of $\bar{G}_2(d_2)$ with degree equal to or greater than

$$\operatorname{int}\deg\begin{bmatrix}G_2(d_2)\\ I_{\ell_1+1}\end{bmatrix}.$$

Consider $i_1<i_2<\cdots<i_s$ and $j_1<j_2<\cdots<j_s$ nonnegative integers. We say that $(i_1,i_2,\cdots,i_s)<(j_1,j_2,\cdots,j_s)$ if there exists $r\in\{1,\ldots,s\}$ such that $i_r<j_r$ and $i_\alpha=j_\alpha$, for $\alpha=1,\ldots,r-1$. Let $r_1<r_2<\cdots<r_s$ and $t_1<t_2<\cdots<t_s$, for some $s\leq\ell_1+1$, such that the submatrix of $G_2(d_2)$ constituted by the rows $r_1,r_2,\ldots,r_s$ and the columns $t_1,t_2,\ldots,t_s$ has determinant of degree $\operatorname{int}\deg\begin{bmatrix}G_2(d_2)\\ I_{\ell_1+1}\end{bmatrix}$ and any other minor constituted by the same rows an by columns $\tilde{t}_1,\tilde{t}_2,\ldots,\tilde{t}_s$ with $(\tilde{t}_1,\tilde{t}_2,\ldots,\tilde{t}_s)<(t_1,t_2,\ldots,t_s)$, has lower degree than the previous one. Moreover, let $j^*$ be such that

$$\deg p_{j^*}(d_2)=\max\{\deg p_j(d_2)\mid j=0,\ldots,\nu_1\}$$

and $\deg p_j(d_2)<\deg p_{j^*}(d_2)$, for $j<j^*$.

Consider now the matrix $M(d_2)$ constituted by the rows $r_1,r_2,\ldots,r_s$ and by the columns $t_1+j^*,t_2+j^*,\ldots,t_s+j^*$ of $\bar{G}_2(d_2)$. Since the $i$-th column of $\bar{G}_2(d_2)$ is equal to

$$\sum_{\{f,\,g\in\mathbb{N}|\ f\leq\ell_1,\,g\leq\nu_1,\,f+g=i-1\}}C_f(d_2)p_g(d_2),$$

for $i=1,\ldots,\ell_1+\nu_1+1$, we have that $\det M(d_2)$ can be written as a sum of minors of the form

$$\prod_{i=1}^{s}p_{y_i}(d_2)\det\begin{bmatrix}\tilde{C}_{t_1+j^*-1-y_1}(d_2) & \tilde{C}_{t_2+j^*-1-y_2}(d_2) & \cdots & \tilde{C}_{t_s+j^*-1-y_s}(d_2)\end{bmatrix},\tag{4.3}$$

where $y_i \in \{0,\dots,\nu_1\}$ and $\tilde{C}_{t_i+j^*-1-y_i}(d_2)$ is the submatrix of $C_{t_i+j^*-1-y_i}(d_2)$ constituted by the rows $r_1, r_2, \dots, r_s$, if $0 \leq t_i + j^* - 1 - y_i \leq \ell_1$, and $\tilde{C}_{t_i+j^*-1-y_i}(d_2) = 0$ otherwise.

Note that, for $i \in \{1,\dots,s\}$, if $0 \leq t_i + j^* - 1 - y_i \leq \ell_1$, then

$$\det \begin{bmatrix} \tilde{C}_{t_1+j^*-1-y_1}(d_2) & \tilde{C}_{t_2+j^*-1-y_2}(d_2) & \cdots & \tilde{C}_{t_s+j^*-1-y_s}(d_2) \end{bmatrix}$$

can be a minor (or the symmetric of a minor) of $G_2(d_2)$, or zero, if it has two identical columns. Moreover,

$$p_{j^*}^s(d_2) \det \begin{bmatrix} \tilde{C}_{t_1-1}(d_2) & \tilde{C}_{t_2-1}(d_2) & \cdots & \tilde{C}_{t_s-1}(d_2) \end{bmatrix} \tag{4.4}$$

is a minors in (4.3) and since $\deg p_{j^*}^s(d_2) \geq \deg p_{y_1}(d_2)p_{y_2}(d_2)\cdots p_{y_s}(d_2)$ for any $y_i \in \{0,\dots,\nu_1\}$ and the degree of

$$\det \begin{bmatrix} \tilde{C}_{t_1-1}(d_2) & \tilde{C}_{t_2-1}(d_2) & \cdots & \tilde{C}_{t_s-1}(d_2) \end{bmatrix}$$

is equal to $\operatorname{int}\deg \begin{bmatrix} G_2(d_2) \\ I_{\ell_1+1} \end{bmatrix}$, then (4.4) has maximum degree among all minors of the form (4.3). We show now that (4.4) has greater degree than the other minors of the form (4.3). In order to do so, we divide the minors (4.3) in two different classes:

1) First we consider the minors (4.3) which are such that there exists $i \in \{1,\dots,s\}$ such that $y_i < j^*$. In this case, $\deg p_{y_i}(d_2) < \deg p_{j^*}(d_2)$, and therefore the degree of (4.3) is smaller than the degree of (4.4).

2) Second we consider the minors (4.3) which are such that $y_i \geq j^*$ for all $i \in \{1,\dots,s\}$ and there exists $i^* \in \{1,\dots,s\}$ such that $y_{i^*} > j^*$ and $y_i = j^*$, for $i < i^*$. In this case, $t_i + j^* - 1 - y_i = t_i - 1$, for $i < i^*$ and $t_{i^*} + j^* - 1 - y_{i^*} < t_{i^*} - 1$ which means that

$$(t_1 + j^* - 1 - y_1, \dots, t_s + j^* - 1 - y_s) < (t_1 - 1, \dots, t_s - 1)$$

and therefore

$$\deg \det \begin{bmatrix} C_{t_1+j^*-1-y_1}(d_2) & \dots & C_{t_s+j^*-1-y_s}(d_2) \end{bmatrix}$$

is smaller then

$$\deg \det \begin{bmatrix} C_{t_1-1}(d_2) & \cdots & C_{t_s-1}(d_2) \end{bmatrix}$$

and consequently (4.3) has degree smaller than (4.4). Thus

$$\deg \det M(d_2) \geq \operatorname{int} \deg \begin{bmatrix} G_2(d_2) \\ I_{\ell_1+1} \end{bmatrix}.$$

To see that $\mu_R(\bar{G}) \geq \mu_R(G)$ let us factorize

$$G(d_1,d_2)p(d_1,d_2) = \hat{G}_2(d_2)\hat{G}_1(d_1)$$

as in Theorem 3.23 in such a way that $M(d_2)$ is a submatrix of $\hat{G}_2(d_2)$. Write

$$\bar{G}_2(d_2) = \left[ I_n \;\middle|\; I_n d_2 \;\middle|\; \cdots \;\middle|\; I_n d_2^{\ell_2+\nu_2} \right] \bar{N},$$

where $\bar{N}$ is a constant matrix.

Note that since the columns $t_1+j^*, t_2+j^*, \ldots, t_s+j^*$ of $\bar{G}_2(d_2)$ are linearly independent over $\mathbb{F}[d_1,d_2]$, then also the columns $t_1+j^*, t_2+j^*, \ldots, t_s+j^*$ of $\bar{N}$ are linearly independent over $\mathbb{F}$, which means that there exists a full column rank constant matrix $\hat{N}_2$ which has the $t_1+j^*, t_2+j^*, \ldots, t_s+j^*$ columns of $\bar{N}$ as a submatrix and a full row rank constant matrix $\hat{N}_1$ such that $\bar{N} = \hat{N}_2\hat{N}_1$. Thus

$$G(d_1,d_2)p(d_1,d_2) = \hat{G}_2(d_2)\hat{G}_1(d_1),$$

where

$$\hat{G}_2(d_2) = \left[ I_n \;\middle|\; I_n d_2 \;\middle|\; \cdots \;\middle|\; I_n d_2^{\ell_2+\nu_2} \right] \hat{N}_2$$

and

$$\hat{G}_1(d_1) = \hat{N}_1 \begin{bmatrix} 1 & d_1 & \cdots & d_1^{\ell_1+\nu_1} \end{bmatrix}^T$$

are such that

$$\mu_R(\bar{G}) = \operatorname{int\,deg} \begin{bmatrix} \hat{G}_2(d_2) \\ I_{\ell_1+\nu_1+1} \end{bmatrix} + \operatorname{int\,deg}(\hat{G}_1(d_1))$$

and $M(d_2)$ is a submatrix of $\hat{G}_2(d_2)$. Thus, since $\det M(d_2)$ is a minor of $\hat{G}_2(d_2)$ and

$$\operatorname{int\,deg}(\hat{G}_1(d_1)) = \operatorname{int}(\deg G_1(d_1)) + \nu_1,$$

we have that

$$\mu_R(\bar{G}) \geq \operatorname{int\,deg} \begin{bmatrix} G_2(d_2) \\ I_{\ell_1+1} \end{bmatrix} + \operatorname{int\,deg}(G_1(d_1)) = \mu_R(G).$$

**Case 2** $N$ is not full column rank.

Then there exists an upper triangular matrix $T$ with 1's in the diagonal such that $N = \tilde{N}_2 T$, where $\tilde{N}_2$ is obtained from $N$ by substituting a column $i$ by zero if it is linear combination of the columns $1,\ldots,i-1$. Let $i_1 < i_2 < \cdots < i_p$ be the nonzero columns of $\tilde{N}_2$, where $p = \operatorname{rank} \tilde{N}_2$. Then $N = N_2 N_1$ where $N_2$ is the full column rank constituted by the columns $i_1, i_2, \ldots, i_p$ of $\tilde{N}_2$ and $N_1$ is the full row rank matrix constituted by the rows $i_1, i_2, \ldots, i_p$ of $T$. Thus $G(d_1, d_2) = G_2(d_2)G_1(d_1)$ where

$$G_2(d_2) = \left[ I_n \;\middle|\; I_n d_2 \;\middle|\; \cdots \;\middle|\; I_n d_2^{\ell_2} \right] N_2$$

and

$$G_1(d_1) = \begin{bmatrix} d_1^{i_1-1}\left(1 + a_1^1 d_1 + a_2^1 d_1^2 + \cdots + a_{\ell_1-(i_1-1)}^1 d_1^{\ell_1-(i_1-1)}\right) \\ d_1^{i_2-1}\left(1 + a_1^2 d_1 + a_2^2 d_1^2 + \cdots + a_{\ell_1-(i_2-1)}^2 d_1^{\ell_1-(i_2-1)}\right) \\ \vdots \\ d_1^{i_p-1}\left(1 + a_1^p d_1 + a_2^p d_1^2 + \cdots + a_{\ell_1-(i_p-1)}^1 d_1^{\ell_1-(i_p-1)}\right) \end{bmatrix},$$

for some $a_j^t \in \mathbb{F}$, for $t = 1,\ldots,p$, $j = 1,\ldots,\ell_1 - (i_t - 1)$. Then

$$G(d_1, d_2)p(d_1, d_2) = \bar{G}_2(d_2)\bar{G}_1(d_1),$$

where $\bar{G}_2(d_2) = G_2(d_2)P(d_2)$, with $P(d_2)$ a $p \times (\ell_1 + \nu_1 + 1)$ matrix such that the $j$-th row is given by

$$\left[ 0_{1\times(i_j-1)} \quad p_0^j(d_2) \quad p_1^j(d_2) \quad \cdots \quad p_{\ell_1+\nu_1-(i_j-1)}^j(d_2) \right],$$

where $p_r^j(d_2) = p_r(d_2) + \sum_{s=1}^{r} a_s^j p_{r-s}(d_2)$, considering $p_r(d_2) = 0$ if $r > \nu_1$, $a_s^j = 0$ if $s > \ell_1 - (i_j - 1)$ and $p_{r-s}(d_2) = 0$ if $r - s > \nu_1$, for $j = 1, \ldots, p$; and $\bar{G}_1(d_1) = \begin{bmatrix} 1 & \cdots & d_1^{\ell_1+\nu_1} \end{bmatrix}^T$.

Similarly to **Case 1** there also exits a minor of $\bar{G}_2(d_2)$ with degree greater or equal than $\operatorname{int\,deg} \begin{bmatrix} G_2(d_2) \\ I_p \end{bmatrix}$. Moreover, in this case, the matrix $M(d_2)$ to be considered is constituted by the rows $r_1, \ldots, r_s$ and the columns $i_{t_1} + j^*, \ldots, i_{t_s} + j^*$ of $\bar{G}_2(d_2)$.

Note that if $j^*$ is such that

$$\deg p_{j^*}(d_2) = \max\{\deg p_i(d_2) \mid i = 0, \ldots, \nu_1\}$$

and $\deg p_i(d_2) < \deg p_{j^*}(d_2)$, for $i < j^*$ then $\deg p_{j^*}^j(d_2) = \max\{\deg p_i^j(d_2) \mid i = 0, \ldots, \nu_1\}$ and $\deg p_i^j(d_2) < \deg p_{j^*}^j(d_2)$, for $i < j^*$.

Applying a similar reasoning as in **Case 1**, we conclude that also in this case $\mu_R(\bar{G}) \geq \mu_R(G)$. □

The following corollary follows immediately from the proof of Theorem 4.1.

**Corollary 4.2.** *Let $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n \times 1}$ be an encoder of a 2D convolutional code with a minimal realization of dimension m, and $p(d_1, d_2) \in \mathbb{F}[d_1, d_2]$ such that, for some $r_1 \in \mathbb{N}$,*

$$p(d_1, d_2) = p_0(d_2) + p_1(d_2)d_1 + p_2(d_2)d_1^2 + \cdots + p_{r_1}(d_2)d_1^{r_1},$$

*with $p_i(d_2) \in \mathbb{F}[d_2]$, $i = 0, \ldots, r_1$ and $p_{r_1}(d_2) \neq 0$. Define $r_2 = \max_{0 \leq i \leq r_1} \deg p_i(d_2)$. Then the minimal dimension of the realization of $\bar{G}(d_1, d_2) = G(d_1, d_2)p(d_1, d_2)$ is equal to or greater than $m + r_1 + r_2$. Moreover, consider $G(d_1, d_2) = G_2(d_2)G_1(d_1)$ a factorization of $G(d_1, d_2)$ as in Theorem 3.23. If $G_2(d_2)$ is row reduced, then a minimal realization of $\bar{G}(d_1, d_2)$ has dimension $m + nr_2 + r_1$.*

*Example* 4.3. Let

$$G(d_1, d_2) = \begin{bmatrix} 1 + d_1^2 + d_1 d_2 + d_2 d_1^2 \\ 1 + 2d_1 + 3d_1^2 + 1d_1^2 d_2 + d_1 d_2 + d_2 \end{bmatrix}$$

be the encoder presented in Example 3.24 which minimal realizations have dimension 4 and consider the equivalent encoder $\bar{G}(d_1, d_2) = G(d_1, d_2)(1 + d_1^2 + d_1 d_2)$. Since $G_2(d_2)$ obtained

in Example 3.24 is row reduced, by Corollary 4.2 we conclude that

$$\mu_R(\bar{G}) = 8 = 4 + nr_2 + r_1,$$

where $r_2 = 1$ and $r_1 = 2$. ◇

## 4.2 On minimal realizations of 2D convolutional codes of rate $k/n$ , $k > 1$

Generalizing the result presented in the previous section for 2D convolutional codes of rate $k/n$, for $k > 1$, appears to be a very difficult problem.

It is not possible to apply a similar reasoning as considered in the previous section to the case $k > 1$. In fact, as happens in the 1D case, and contrary to what happens in the case $k = 1$, post-multiplication of an encoder $G(d_1, d_2)$ by a nonsingular matrix $P(d_1, d_2)$ can decrease the McMillan degree as next example shows.

*Example* 4.4. Let us consider the following right-factor prime 2D encoder

$$G(d_1,d_2) = \begin{bmatrix} 1 + d_1 - d_1^4 + d_2 + d_1d_2 - d_2d_1^4 & -1 - d_1^4 - d_2 - d_2d_1^4 \\ d_1 + d_1^3 - d_1^4 + d_1d_2 + d_2d_1^3 - d_2d_1^4 & -1 - d_1^3 + d_1^4 - d_2 - d_2d_1^3 + d_2d_1^4 \\ d_1 + d_1^3 & -1 - d_1 - d_1^3 \end{bmatrix}.$$

Rewriting $G(d_1, d_2) = G_2(d_2)G_1(d_1)$ as in Theorem 3.23 , with

$$G_2(d_2) = \begin{bmatrix} 1 + d_2 & 0 & 0 \\ 0 & 1 + d_2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

and

$$G_1(d_1) = \begin{bmatrix} 1 + d_1 - d_1^4 & -1 + d_1^4 \\ d_1 + d_1^3 - d_1^4 & -1 - d_1^3 + d_1^4 \\ d_1 + d_1^3 & -1 - d_1 - d_1^3 \end{bmatrix}$$

it is easy to check that the McMillan degrees of $G_2(d_2)$ and of $G_1(d_1)$ are 2 and 4, respectively.

Moreover, post-multiplying $G(d_1,d_2)$ by a nonsingular matrix $P(d_1) = \begin{bmatrix} d_1^3+1 & -d_1 \\ d_1^3 & -d_1 \end{bmatrix}$ we obtain an equivalent encoder of $G(d_1,d_2)$ given by

$$\begin{aligned} \bar{G}(d_1,d_2) &= G(d_1,d_2)P(d_1) \\ &= \begin{bmatrix} 1+d_1+d_2+d_1d_2 & -d_1^2-d_1^2d_2 \\ d_1+d_1d_2 & d_1-d_1^2-d_1^2d_2+d_1d_2 \\ d_1 & d_1 \end{bmatrix}, \end{aligned}$$

which is not right-factor prime. Rewriting $\bar{G}(d_1,d_2) = \bar{G}_2(d_2)\bar{G}_1(d_1)$ as in Theorem 3.23, with

$$\bar{G}_2(d_2) = G_2(d_2) \quad \text{and} \quad \bar{G}_1(d_1) = \begin{bmatrix} d_1+1 & -d_1^2 \\ d_1 & -d_1^2+d_1 \\ d_1 & d_1 \end{bmatrix}$$

it is easy to check that the McMillan degree of $\bar{G}_1(d_1)$ is 3. Therefore

$$\mu_R(\bar{G}) = \mu(\bar{G}_2) + \mu(\bar{G}_1) < \mu(G_2) + \mu(G_1) = \mu_R(G).$$

◇

The previous example also allows to conclude that extracting a factor ($P$) to a non right-factor prime encoder ($\bar{G}$), in order to make it a right-factor prime one ($G$), does not necessarily decrease the $R$-McMillan degree.

However in some cases, given an encoder of a 2D convolutional code $C$ it is possible to obtain an equivalent encoder of smaller McMillan degree. The next result is a first step in that direction.

**Lemma 4.5.** *Let $G(d_1,d_2) \in \mathbb{F}[d_1,d_2]^{n\times k}$ be a polynomial encoder of a convolutional code of rate $k/n$, with R-McMillan degree $\mu_R(G)$. Let also $G(d_1,d_2) = G_2(d_2)G_1(d_1)$ be a factorization of $G(d_1,d_2)$ as in Theorem 3.23. Consider an equivalent encoder of $G(d_1,d_2)$, $\bar{G}(d_1,d_2)$, such that*

$$\bar{G}(d_1,d_2) = G_2(d_2)G_1(d_1)P(d_1), \tag{4.5}$$

*where $P(d_1)$ is an arbitrary nonsingular polynomial matrix only in the indeterminate $d_1$, i.e., $P(d_1) = P_0 + P_1 d_1 + \cdots + P_\delta d_1^\delta \in \mathbb{F}[d_1]^{k\times k}$, for some $\delta \in \mathbb{N}$ and $P_i \in \mathbb{F}^{k\times k}$, $i = 0, 1, \ldots, \delta$. Then the Roesser McMillan degree of $\bar{G}(d_1, d_2)$ is given by $\mu_R(\bar{G}) = \mu(G_2) + \mu(G_1 P)$.*

*Proof.* Let $G(d_1, d_2) = G_2(d_2)G_1(d_1) \in \mathbb{F}[d_1, d_2]^{n\times k}$ be a polynomial matrix factorized as in (3.39) and $P(d_1)$ a nonsingular polynomial matrix such that $P(d_1) = P_0 + P_1 d_1 + \cdots + P_\delta d_1^\delta \in \mathbb{F}[d_1]^{k\times k}$ for some $\delta \in \mathbb{N}$ and $P_i \in \mathbb{F}^{k\times k}$, $i = 0, 1, \ldots, \delta$. Consider now the equivalent encoder $\bar{G}(d_1, d_2) = G(d_1, d_2)P(d_1)$. Note that $\bar{G}(d_1, d_2)$ can be rewritten as follows,

$$
\begin{aligned}
\bar{G}(d_1, d_2) &= G(d_1, d_2)P(d_1) \\
&= G_2(d_2)G_1(d_1)P(d_1) \\
&= G_2(d_2)N_1 \begin{bmatrix} I_k \\ I_k d_1 \\ \vdots \\ I_k d_1^{\ell_1} \end{bmatrix} P(d_1) \\
&= G_2(d_2)N_1 \begin{bmatrix} P(d_1) \\ P(d_1)d_1 \\ \vdots \\ P(d_1)d_1^{\ell_1} \end{bmatrix} \\
&= G_2(d_2)N_1 \begin{bmatrix} P_0 + P_1 d_1 + \cdots + P_\delta d_1^\delta \\ P_0 d_1 + P_1 d_1^2 + \cdots + P_\delta d_1^{\delta+1} \\ \vdots \\ P_0 d_1^{\ell_1} + P_1 d_1^{\ell_1+1} + \cdots + P_\delta d_1^{\ell_1+\delta} \end{bmatrix} \\
&= G_2(d_2)N_1\mathcal{P} \begin{bmatrix} I_k \\ I_k d_1 \\ \vdots \\ I_k d_1^{\ell_1+\delta} \end{bmatrix},
\end{aligned}
$$

where

$$\mathcal{P} = \begin{bmatrix} P_0 & \cdots & P_\delta & & 0 \\ & \ddots & & \ddots & \\ 0 & & P_0 & \cdots & P_\delta \end{bmatrix},$$

and $G_1(d_1)$ as in (3.41).

Thus

$$\bar{G}(d_1, d_2) = G_2(d_2)\bar{G}_1(d_1), \tag{4.6}$$

with $G_2(d_2)$ as in (3.40) and

$$\bar{G}_1(d_1) = G_1(d_1)P(d_1) = N_1\mathcal{P}\begin{bmatrix} I_k \\ I_k d_1 \\ \vdots \\ I_k d_1^{\ell_1+\delta} \end{bmatrix}. \tag{4.7}$$

In order to prove that $\mu_R(\bar{G}) = \mu(G_2) + \mu(\bar{G}_1)$, we have to prove that the decomposition (4.6) is as in Theorem 3.23. For that purpose it is enough to prove that $N_1\mathcal{P}$ is a full row rank constant matrix. To this end, let us now consider the following cases:

(i) $P(d_1)$ is unimodular

If $P(d_1) = P_0 + P_1 d_1 + \cdots + P_\delta d_1^\delta$ is unimodular then $P_0$ is a $k \times k$ invertible constant matrix which implies immediately that $\mathcal{P}$ has full row rank and consequently, as $N_1$ has also full row rank, $N_1\mathcal{P}$ has full row rank, as we wish to prove.

(ii) $P(d_1)$ is not unimodular

If $P(d_1)$ is but not unimodular but still invertible, then there exists a $k \times k$ rational matrix $Q(d_1)$ such that

$$P(d_1)Q(d_1) = I_k, \tag{4.8}$$

with $Q(d_1) = \frac{S(d_1)}{m(d_1)}$, where $S(d_1) = S_0 + S_1 d_1 + \cdots + S_\zeta d_1^\zeta$, for some $\zeta \in \mathbb{N}$ and $S_i \in \mathbb{F}^{k\times k}$, for $i \in \{0, \ldots, \zeta\}$, and $m(d_1) = m_t d_1^t + m_{t+1} d_1^{t+1} + \cdots + m_{t+r} d_1^{t+r}$, with $m_t \neq 0$, for some $t, r \in \mathbb{N}$ and $m_i \in \mathbb{F}$, $i = t, \ldots t + r$. Consider, without loss of generality, $\delta = \zeta$.

Therefore,

$$P(d_1)S(d_1) = I_k m(d_1), \tag{4.9}$$

Hence, we conclude that it is always possible to find a polynomial matrix $S(d_1)$, such that post-multiplying $P(d_1)$ by $S(d_1)$ yields a polynomial matrix which has the first nonzero coefficient matrix invertible, i.e., the product

$$\begin{bmatrix} P_0 & \cdots & P_\delta & & 0 \\ & \ddots & & \ddots & \\ 0 & & P_0 & \cdots & P_\delta \end{bmatrix} \begin{bmatrix} S_\delta & & 0 \\ \vdots & \ddots & \\ S_0 & & S_\delta \\ & \ddots & \vdots \\ 0 & & S_0 \end{bmatrix} = \begin{bmatrix} I_k & & & & * \\ & I_k & & & \\ & & \ddots & & \\ & & & I_k & \\ 0 & & & & I_k \end{bmatrix}$$

This implies that $\mathcal{P}$ has full row rank. Consequently, as $N_1$ has full row rank, $N_1\mathcal{P}$ has also full row rank.

Thus the McMillan degree of $\bar{G}(d_1, d_2)$ is given by $\mu(G_2) + \mu(\bar{G}_1)$, as we wish to prove. □

Now, if $G_1(d_1)$ in (4.5) is already a 1D minimal encoder, it is not possible to reduce its McMillan degree any further and we conclude that $\mu(G_1) \leq \mu(G_1P)$, for any $P(d_1) \in \mathbb{F}[d_1]^{k\times k}$.

In case $G(d_1, d_2) = G_2(d_2)G_1(d_1)$ is such that $G_1(d_1)$ is not a minimal encoder, if there exists $P(d_1) \in \mathbb{F}[d]^{k\times k}$ such that $\bar{G}_1(d_1) = G_1(d_1)P(d_1)$ is a canonical encoder equivalent to $G_1(d_1)$, it follows that

$$\bar{G}(d_1, d_2) = G(d_1, d_2)P(d_1) = G_2(d_2)\bar{G}_1(d_1)$$

is an equivalent encoder to $G(d_1, d_2)$ such that

$$\mu_R(\bar{G}) = \mu(G_2) + \mu(\bar{G}_1) = \mu(G_2) + \mu(G_1P_1) < \mu(G_2) + \mu(G_1) = \mu_R(G).$$

These considerations allow us to conclude that in some cases we can obtain encoders with lower $R$-McMillan degree than a given encoder $G(d_1, d_2)$, by post-multiplying it by a suitable 1D polynomial matrix $P(d_1)$ such that

$$\mu(G_1P) < \mu(G_1), \tag{4.10}$$

where $G_1(d_1)$ is the right-factor in the decomposition of $G(d_1,d_2) = G_2(d_2)G_1(d_1)$, given by Theorem 3.23. The inequality (4.10) is strict unless $G_1(d_1)$ is itself already a minimal encoder of the corresponding code.

*Example* 4.6. Let us consider an encoder $G(d_1,d_2)$ of a 2D convolutional code $C$ given by

$$G(d_1,d_2) = \begin{bmatrix} d_2d_1(d_1+1) & -d_2(1+d_1+d_1^2) \\ d_2d_1 - d_2d_1^3 + d_2d_1^2 + d_1 + d_1^2 & -1 + d_2d_1^3 - d_2d_1^2 - d_2 - d_1 - d_1^2 \\ 1 + d_1 + d_2d_1 - d_1^3 - d_2d_1^3 + d_2d_1^2 & -1 - d_2 - d_1^3 + d_2d_1^3 - d_2d_1^2 \end{bmatrix}$$

such that it admits a factorization as in Theorem 3.23 given by $G(d_1,d_2) = G_2(d_2)G_1(d_1)$ where

$$G_2(d_2) = \begin{bmatrix} 0 & 0 & d_2 \\ 0 & d_2 & 1 \\ 1 & d_2 & 0 \end{bmatrix}$$

and

$$G_1(d_1) = \begin{bmatrix} 1 + d_1 - d_1^3 & -1 + d_1^3 \\ d_1 + d_1^2 - d_1^3 & -1 - d_1^2 + d_1^3 \\ d_1 + d_1^2 & -1 - d_1 - d_1^2 \end{bmatrix}$$

such that $\mu(G_1) = 3$.

Consider now an equivalent encoder of $G(d_1,d_2)$ given by

$$\bar{G}(d_1,d_2) = G(d_1,d_2)P(d_1) = \bar{G}_2(d_2)\bar{G}_1(d_1),$$

where $P(d_1) = \begin{bmatrix} d_1^2+1 & -1 \\ d_1^2 & -1 \end{bmatrix}$, $\bar{G}_2(d_2) = G_2(d_2)$ and

$$\bar{G}_1(d_1) = \begin{bmatrix} d_1+1 & -d_1 \\ d_1 & -d_1+1 \\ d_1 & 1 \end{bmatrix},$$

with $\bar{G}_1(d_1)$ 1D canonical and such that $\mu(\bar{G}_1) = 2$. Then, it follows that

$$\mu_R(\bar{G}) = \mu(G_2) + \mu(\bar{G}_1) < \mu(G_2) + \mu(G_1) = \mu_R(G).$$

◇

As illustrated in the previous example, in case $G_1(d_1)$ is right-prime, post-multiplication by a unimodular matrix $P(d_1)$ does transform it into a column reduced, and hence into a canonical encoder, decreasing the corresponding McMillan degree in case $G_1(d_1)$ is not minimal. This is stated in the following corollary.

**Corollary 4.7.** *Let $\mathcal{C}$ be a 2D convolutional code and $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$ be an encoder of $\mathcal{C}$. Moreover, let $G(d_1, d_2) = G_2(d_2)G_1(d_1)$ be factorized as in Theorem 3.23, and assume that $G(d_1, d_2)$ is a 2D right-factor prime (rFP) encoder of $\mathcal{C}$ and $G_1(d_1)$ is not a minimal encoder. Then there exists a unimodular matrix $U_1(d_1)$ such that*

$$\mu_R(GU_1) < \mu_R(G).$$

*Proof.* Take $U_1(d_1)$ unimodular such that

$$\bar{G}_1(d_1) = G_1(d_1)U_1(d_1)$$

is column reduced. Clearly $G_1(d_1)$ is right-prime because, by assumption, $G(d_1, d_2)$ is rFP and therefore $\bar{G}_1(d_1)$ is canonical. Then, by Lemma 4.5

$$\mu_R(GU_1) = \mu(G_2) + \mu(G_1U_1) < \mu(G_2) + \mu(G_1) = \mu_R(G).$$

□

However the procedure illustrated in the Example 4.6 cannot always be applied, as there exist 1D encoders $G_1(d_1)$ that are not reducible to canonical ones by post-multiplication by a polynomial matrix $P(d_1)$.

# Chapter 5

# Composition codes

In this chapter we consider a particular class of 2D polynomial encoders and corresponding 2D convolutional codes that we call composition encoders and composition codes. These encoders are obtained through the composition of two 1D encoders, each one in one direction/indeterminate. We prove that under certain conditions, composition encoders are minimal. Moreover, for the encoders that satisfy these minimality conditions, minimal 2D state-space realizations are obtained, which are minimal realizations of the corresponding 2D convolutional codes.

## 5.1 Composition encoders and composition codes

The formal definition of composition encoders is as follows.

**Definition 5.1.** An encoder $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n \times k}$ such that

$$G(d_1, d_2) = G_2(d_2)G_1(d_1),$$

where $G_1(d_1) \in \mathbb{F}[d_1]^{p \times k}$ and $G_2(d_2) \in \mathbb{F}[d_2]^{n \times p}$ are 1D encoders, is said to be a *composition encoder*.

Note that the requirement that $G_i(d_i)$, for $i = 1, 2$, is a 1D encoder is equivalent to the condition that $G_i(d_i)$ is a full column rank matrix. Moreover this requirement clearly implies

that $G_2(d_2)G_1(d_1)$ has full column rank, hence the composition $G_2G_1$ of two 1D encoders is indeed a 2D encoder.

The 2D composition code $\mathcal{C}$ associated with $G(d_1,d_2) = G_2(d_2)G_1(d_1)$ is given as

$$\begin{aligned}\mathcal{C} &= \text{Im } G(d_1,d_2) = G_2(d_2)(\text{Im}(G_1(d_1)))\\ &= \{\hat{w}(d_1,d_2) \in \mathcal{F}_{2D}^n : \exists\ \hat{z}(d_1,d_2) \in \text{Im } (G_1(d_1)) \text{ such that}\\ &\quad \hat{w}(d_1,d_2) = G_2(d_2)\hat{z}(d_1,d_2)\}.\end{aligned}$$

Next we restrict our study to 2D composition encoders that admit a special structure, namely, in which $G_2(d_2)$ is a quasi-systematic encoder, (cf. Definition 2.8).

Observe that quasi-systematic encoders are right-prime, but not necessarily column reduced, and hence they are not necessarily canonical. However as stated in the following proposition they are minimal encoders. Although this is a well-known result [9, 11], we present here a different proof that uses the results and tools from Chapter 3.

**Proposition 5.2.** *Let $G(d) \in \mathbb{F}[d]^{n\times k}$ be a polynomial encoder. If $G(d)$ is quasi-systematic then every minimal realization of $G(d)$ is a minimal realization of $\mathcal{C} = \text{Im } G(d)$.*

Before proving the proposition we state some auxiliary results.

**Lemma 5.3.** *If $\bar{\Sigma}^{1D}(\bar{A},\bar{B},\bar{C},\bar{D})$ is a minimal realization of an encoder $\bar{G}(d) \in \mathbb{F}[d]^{(n-k)\times k}$ then $\Sigma^{1D}\left(\bar{A},\bar{B},\begin{bmatrix}\bar{C}\\0\end{bmatrix},\begin{bmatrix}\bar{D}\\I_k\end{bmatrix}\right)$ is a minimal realization of the encoder $\begin{bmatrix}\bar{G}(d)\\I_k\end{bmatrix} \in \mathbb{F}[d]^{n\times k}$.*

*Proof.* Clearly, if the pair $(\bar{A},\bar{C})$ is observable then $\left(\bar{A},\begin{bmatrix}\bar{C}\\0\end{bmatrix}\right)$ is observable. Since the minimality of an encoder realization is equivalent to its controllability and observability, and the pair $(\bar{A},\bar{B})$ is the same for both realizations, the result follows immediately. □

**Lemma 5.4.** *(Corollary of Lemma 5.3) Every minimal realization of an encoder $\begin{bmatrix}\bar{G}(d)\\I_k\end{bmatrix} \in \mathbb{F}[d]^{n\times k}$ is of the form $\Sigma^{1D}\left(\tilde{A},\tilde{B},\begin{bmatrix}\tilde{C}\\0\end{bmatrix},\begin{bmatrix}\tilde{D}\\I_k\end{bmatrix}\right)$, where $\tilde{\Sigma}^{1D}(\tilde{A},\tilde{B},\tilde{C},\tilde{D})$ is a minimal realization of $\bar{G}(d) \in \mathbb{F}[d]^{(n-k)\times k}$.*

*Proof.* Let $\bar{\Sigma}^{1D}(\bar{A},\bar{B},\bar{C},\bar{D})$ be a minimal realization of $\bar{G}(d)$. Then, by Lemma 5.3,

$$\Sigma_*^{1D}\left(\bar{A},\bar{B},\begin{bmatrix}\bar{C}\\0\end{bmatrix},\begin{bmatrix}\bar{D}\\I_k\end{bmatrix}\right)$$

is a minimal realization of $\begin{bmatrix}\bar{G}(d)\\I_k\end{bmatrix}$. Since all the minimal realizations of $\bar{G}(d)$ are equivalent, these realizations are of the form:

$$\Sigma_S^{1D}\left(S\bar{A}S^{-1},S\bar{B},\begin{bmatrix}\bar{C}\\0\end{bmatrix}S^{-1},\begin{bmatrix}\bar{D}\\I_k\end{bmatrix}\right)=\Sigma_S^{1D}\left(\tilde{A},\tilde{B},\begin{bmatrix}\tilde{C}\\0\end{bmatrix},\begin{bmatrix}\tilde{D}\\I_k\end{bmatrix}\right),$$

where $\tilde{A}=S\bar{A}S^{-1}$, $\tilde{B}=S\bar{B}$, $\tilde{C}=\bar{C}S^{-1}$, $\tilde{D}=\bar{D}$ with $S$ an invertible constant matrix.

Clearly $\tilde{\Sigma}^{1D}(\tilde{A},\tilde{B},\tilde{C},\tilde{D})$ is a minimal realization of $\bar{G}(d)$, proving that every minimal realization of $\begin{bmatrix}\bar{G}(d)\\I_k\end{bmatrix}$ has the desired form. □

**Proof of Proposition 5.2.**

*Proof.* Let $G(d)$ be a quasi-systematic encoder. Without loss of generality assume that $G(d)=\begin{bmatrix}\bar{G}(d)\\I\end{bmatrix}$ (otherwise multiply $G(d)$ by a suitable invertible matrix $T^{-1}$, and then multiply the output matrices of the realization by $T$.)

Let $\Sigma^{1D}(A,B,C,D)$ be a minimal realization of $G(d)$ of dimension $m$. Then by Lemma 5.4, $C=\begin{bmatrix}\bar{C}\\0\end{bmatrix}$ and $D=\begin{bmatrix}\bar{D}\\I_k\end{bmatrix}$, where $\bar{\Sigma}^{1D}(A,B,\bar{C},\bar{D})$ is a minimal realization of $\bar{G}(d)$ (also of dimension $m$). This means that $(A,B)$ is controllable and $(A,\bar{C})$ is observable.

Next we show that Willems's conditions given in Theorem 3.9 for the minimality of $\Sigma^{1D}(A,B,C,D)$ as a realization of $C=\operatorname{Im}G(d)$ are satisfied.

Condition (i) is obviously satisfied because $D=\begin{bmatrix}\bar{D}\\I_k\end{bmatrix}$ and therefore $\begin{bmatrix}B\\D\end{bmatrix}$ has full column rank.

Regarding the condition (ii), this condition is clearly satisfied due to the controllability of $(A,B)$.

As for conditions (iii) and (iv), note that $B = LD$, with $L = \begin{bmatrix} 0 & B \end{bmatrix}$, and that $\Lambda = \begin{bmatrix} I_{n-k} & -\bar{D} \end{bmatrix}$ is a *mla* of $D$. Thus, recalling that $C = \begin{bmatrix} \bar{C} \\ 0 \end{bmatrix}$:

$$A - LC = A - \begin{bmatrix} 0 & B \end{bmatrix} \begin{bmatrix} \bar{C} \\ 0 \end{bmatrix} = A$$

and

$$\Lambda C = \begin{bmatrix} I & -\bar{D} \end{bmatrix} \begin{bmatrix} \bar{C} \\ 0 \end{bmatrix} = \bar{C},$$

i.e.,

$$(A - LC, \Lambda C) = (A, \bar{C}),$$

which is clearly observable due to the fact that $\bar{\Sigma}^{1D}(A, B, \bar{C}, \bar{D})$ is a minimal realization.

Therefore we conclude that $\Sigma^{1D}(A, B, C, D)$ is also a minimal realization of $\mathcal{C} = \text{Im } G(d)$.

□

*Example* 5.5. Consider the polynomial encoder given by

$$G(d) = \begin{bmatrix} d & 1 & d & 0 \\ 0 & d^2 & 0 & d^2 \\ d+1 & 0 & d+1 & 0 \\ 0 & d^2+1 & 0 & d^2+1 \\ 1 & 1 & 0 & 0 \\ d & d^2 & d & d^2 \end{bmatrix}.$$

$G(d)$ is a quasi-systematic encoder since

$$G(d) = T \begin{bmatrix} \bar{G}(d) \\ I_4 \end{bmatrix},$$

with $T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$ invertible and $\bar{G}(d) = \begin{bmatrix} d & 0 & d & 0 \\ 0 & d^2 & 0 & d^2 \end{bmatrix}$.

Since

$$\Sigma^{1D}\left(\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}\right)$$

is a 1D minimal realization of $G(d)$, it is a minimal realization of the corresponding code as well. This can also be confirmed by checking the conditions of Theorem 3.9. ◇

## 5.2 Minimal realizations of composition codes

In this section we consider composition codes generated by composition encoders

$$G(d_1, d_2) = G_2(d_2)G_1(d_1),$$

where $G_2(d_2)$ is quasi-systematic. We prove that, in this case, the composition code Im $G(d_1, d_2)$ has a minimal 2D state-space realization by means of a separable Roesser model that can be obtained from minimal state-space realizations of the 1D convolutional codes Im $G_1(d_1)$ and Im $G_2(d_2)$ .

Let then $\mathcal{C}$ be a composition code generated by a composition encoder $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{q\times k}$ such that

$$G(d_1, d_2) = G_2(d_2)G_1(d_1), \tag{5.1}$$

where $G_2(d_2) \in \mathbb{F}[d_2]^{n\times p}$, for some $p \in \mathbb{N}$, is a quasi-systematic encoder, and $G_1(d_1) \in \mathbb{F}[d_1]^{p\times k}$ is a minimal encoder. Note that the minimality assumption on $G_1(d_1)$ is not restric-

tive, as $G_1(d_1)$ can be taken to be right-prime and post-multiplying $G(d_1,d_2)$ by a suitable unimodular matrix $U(d_1)$ allows putting $G_1(d_1)$ in the column reduced form, without changing the corresponding code. Let $\Sigma^{1D}(A_{11},B_1,\bar{C}_1,\bar{D}_1)$ and $\Sigma^{1D}(A_{22},\bar{B}_2,C_2,\bar{D}_2)$ be minimal realizations of $G_1(d_1)$ and $G_2(d_2)$, respectively. Observe that, since $G_1(d_1)$ is a minimal encoder, $\Sigma^{1D}(A_{11},B_1,\bar{C}_1,\bar{D}_1)$ is a minimal realization of the 1D code $C_1 = \text{Im } G_1(d_1)$. Moreover, by Proposition 5.2, because $G_2(d_2)$ is quasi-systematic, $\Sigma^{1D}(A_{22},\bar{B}_2,C_2,\bar{D}_2)$ is a minimal realization of the 1D convolutional code $C_2 = \text{Im } G_2(d_2)$.

Connecting in series $\Sigma^{1D}(A_{11},B_1,\bar{C}_1,\bar{D}_1)$ and $\Sigma^{1D}(A_{22},\bar{B}_2,C_2,\bar{D}_2)$ yields the following 2D realization of $G(d_1,d_2)$:

$$\begin{cases} \sigma_1 x_1 = A_{11}x_1 + B_1 u \\ \sigma_2 x_2 = A_{21}x_1 + A_{22}x_2 + B_2 u \\ w = C_1 x_1 + C_2 x_2 + Du, \end{cases} \tag{5.2}$$

where $A_{21} = \bar{B}_2\bar{C}_1$, $B_2 = \bar{B}_2\bar{D}_1$, $C_1 = \bar{D}_2\bar{C}_1$ and $D = \bar{D}_2\bar{D}_1$.

As we shall see, under the assumption that $\begin{bmatrix}\bar{C}_1 & \bar{D}_1\end{bmatrix}$ is invertible, the minimality of $\Sigma^{1D}(A_{11},B_1,\bar{C}_1,\bar{D}_1)$ and $\Sigma^{1D}(A_{22},\bar{B}_2,C_2,\bar{D}_2)$ implies that the realizations $\Sigma^{1D}(A_{11},B_1,E,F)$ and $\Sigma^{1D}(A_{22},J,C_2,H)$, with

$$E = \begin{bmatrix}A_{21}\\ C_1\end{bmatrix} = \begin{bmatrix}\bar{B}_2\\ \bar{D}_2\end{bmatrix}\bar{C}_1, \quad F = \begin{bmatrix}B_2\\ D\end{bmatrix} = \begin{bmatrix}\bar{B}_2\\ \bar{D}_2\end{bmatrix}\bar{D}_1$$

and

$$J = \begin{bmatrix}A_{21} & B_2\end{bmatrix} = \bar{B}_2\begin{bmatrix}\bar{C}_1 & \bar{D}_1\end{bmatrix}, \quad H = \begin{bmatrix}C_1 & D\end{bmatrix} = \bar{D}_2\begin{bmatrix}\bar{C}_1 & \bar{D}_1\end{bmatrix},$$

are minimal code realizations that satisfy the sufficient conditions for minimality of Theorem 3.9.

By Theorem 3.30, this in turn allows to conclude that the realization

$$\Sigma^{2D}(A_{11},A_{21},A_{22},B_1,B_2,C_1,C_2,D)$$

given by (5.2) is a minimal realization of the composition code $C$, as stated in the following result.

**Theorem 5.6.** *Let $G(d_1, d_2) \in \mathbb{F}[d_1, d_2]^{n\times k}$ be a composition encoder such that*

$$G(d_1, d_2) = G_2(d_2)G_1(d_1),$$

*where $G_2(d_2) \in \mathbb{F}[d_2]^{n\times p}$ is quasi-systematic and $G_1(d_1) \in \mathbb{F}[d_1]^{p\times k}$, for some $p \in \mathbb{N}$, is a minimal 1D encoder. Moreover, let $\Sigma^{1D}(A_{11}, B_1, \bar{C}_1, \bar{D}_1)$ and $\Sigma^{1D}(A_{22}, \bar{B}_2, C_2, \bar{D}_2)$ be two 1D minimal realization of $G_2(d_2)$ and $G_1(d_1)$, respectively, and assume that $\begin{bmatrix}\bar{C}_1 & \bar{D}_1\end{bmatrix}$ is square and invertible.*

*Then $\Sigma^{2D}(A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D)$, where $A_{21} = \bar{B}_2\bar{C}_1$, $B_2 = \bar{B}_2\bar{D}_1$, $C_1 = \bar{D}_2\bar{C}_1$ and $D = \bar{D}_2\bar{D}_1$ is a minimal realization of $C$.*

*Proof.* Let $\Sigma^{1D}(A_{11}, B_1, \bar{C}_1, \bar{D}_1)$ and $\Sigma^{1D}(A_{22}, \bar{B}_2, C_2, \bar{D}_2)$ be both 1D minimal realizations of Im $G_1(d_1)$ and Im $G_2(d_2)$, respectively. By Theorem 3.9 (and the remark thereafter) this means that:

Condition 1: $\bar{D}_1$ and $\bar{D}_2$ have full column rank.

Condition 2: $(A_{11}, B_1)$ and $(A_{22}, \bar{B}_2)$ are both controllable pairs.

Condition 3: $\ker \bar{D}_1 \subseteq \ker B_1$ and $\ker \bar{D}_2 \subseteq \ker \bar{B}_2$ (i.e, there exist matrices $L_1$ and $L_2$ such that $B_1 = L_1\bar{D}_1$ and $\bar{B}_2 = L_2\bar{D}_2$ ).

Condition 4: Let $L_1$ and $L_2$ be defined as in Condition 3, and let $\Lambda_1$ and $\Lambda_2$ be minimal left-annihilators (mla) of $\bar{D}_1$ and $\bar{D}_2$, respectively. Then the pairs $(A_{11} - L_1\bar{C}_1, \Lambda_1\bar{C}_1)$ and $(A_{22} - L_2C_2, \Lambda_2C_2)$ are both observable.

Firstly we show that the conditions of Theorem 3.9 for the minimality of $\Sigma^{1D}(A_{11}, B_1, E, F)$ as a code realization are satisfied. For this purpose we prove that:

(i) $F$ has full column rank

Since Condition 1 and Condition 3 hold,

$$F = \begin{bmatrix}\bar{B}_2\\ \bar{D}_2\end{bmatrix}\bar{D}_1 = \begin{bmatrix}L_2\\ I\end{bmatrix}\bar{D}_2\bar{D}_1$$

has full column rank as its factors $\bar{D}_1$, $\bar{D}_2$ and $\begin{bmatrix} L_2 \\ I \end{bmatrix}$ have full column rank.

(ii) $(A_{11}, B_1)$ is controllable

This condition trivially holds due to Condition 2, i.e., $(A_{11}, B_1)$ is a controllable pair.

(iii) There exists a matrix $\bar{L}_1$ such that $B_1 = \bar{L}_1 F$

Taking into account that

$$F = \begin{bmatrix} B_2 \\ D \end{bmatrix}, \; D = \bar{D}_2 \bar{D}_1 \;\text{ and } B_2 = \bar{B}_2 \bar{D}_1, \tag{5.3}$$

the claim to be shown is equivalent to the existence of a matrix $\bar{L}_1$ such that

$$B_1 = \bar{L}_1 \begin{bmatrix} \bar{B}_2 \bar{D}_1 \\ \bar{D}_2 \bar{D}_1 \end{bmatrix} = \bar{L}_1 \begin{bmatrix} \bar{B}_2 \\ \bar{D}_2 \end{bmatrix} \bar{D}_1. \tag{5.4}$$

Since, by Conditions 1 and 3, $\bar{B}_2 = L_2 \bar{D}_2$ and $\bar{D}_2$ has full column rank, respectively, $\begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2$ has full column rank and then, there exists a left inverse, $U$, such that

$$U \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 = I. \tag{5.5}$$

On the other hand, there exists $L_1$ such that $B_1 = L_1 \bar{D}_1$. Therefore, from (5.3), (5.4) and (5.5) we obtain that

$$B_1 = \bar{L}_1 F, \tag{5.6}$$

where $\bar{L}_1 = L_1 U$.

(iv) $(A_{11} - \bar{L}_1 E, \bar{\Lambda}_1 E)$ is observable, with $\bar{L}_1$ s.t. $B_1 = \bar{L}_1 F$ and $\bar{\Lambda}_1$ is a *mla* of $F$

To prove this, consider $\bar{L}_1 = L_1 U$, as defined above. Moreover note that

$$\Lambda_1 U F = \Lambda_1 U \begin{bmatrix} \bar{B}_2 \\ \bar{D}_2 \end{bmatrix} \bar{D}_1 = \Lambda_1 U \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 \bar{D}_1 = \Lambda_1 \bar{D}_1 = 0$$

due to (5.5) and to the fact that $\Lambda_1$ is, by definition, a *mla* of $\bar{D}_1$.

This implies that a *mla* of $F$ can be obtained by (if necessary) adding extra rows to $\Lambda_1 U$.

Let then $\bar{\Lambda}_1 = \begin{bmatrix} \Lambda_1 U \\ T \end{bmatrix}$, for a suitable matrix $T$, be a *mla* of $F$. Now,

$$\begin{aligned}
(A_{11} - \bar{L}_1 E, \bar{\Lambda}_1 E) &= \left( A_{11} - \bar{L}_1 \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 \bar{C}_1, \bar{\Lambda}_1 \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 \bar{C}_1 \right) \\
&= \left( A_{11} - L_1 U \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 \bar{C}_1, \begin{bmatrix} \Lambda_1 U \\ T \end{bmatrix} \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 \bar{C}_1 \right) \\
&= \left( A_{11} - L_1 \bar{C}_1, \begin{bmatrix} \Lambda_1 \bar{C}_1 \\ M \end{bmatrix} \right),
\end{aligned}$$

where $M = T \begin{bmatrix} L_2 \\ I \end{bmatrix} \bar{D}_2 \bar{C}_1$.

Since, by Condition 4, the pair $(A_{11} - L_1 \bar{C}_1, \Lambda_1 \bar{C}_1)$ is observable, then the pair

$$\left( A_{11} - L_1 \bar{C}_1, \begin{bmatrix} \Lambda_1 \bar{C}_1 \\ M \end{bmatrix} \right)$$

is also observable. In this way we conclude that $(A_{11} - \bar{L}_1 E, \bar{\Lambda}_1 E)$ is observable, as desired.

Therefore all the conditions of Theorem 3.9 are satisfied and $\Sigma^{1D}(A_{11}, B_1, E, F)$ is minimal as a code realization.

Finally, note that

$$\Sigma^{1D}(A_{22}, J, C_2, H) = \Sigma^{1D} \left( A_{22}, \bar{B}_2 \begin{bmatrix} \bar{C}_1 & \bar{D}_1 \end{bmatrix}, C_2, \bar{D}_2 \begin{bmatrix} \bar{C}_1 & \bar{D}_1 \end{bmatrix} \right)$$

corresponds to making an invertible input transformation, associated to $\begin{bmatrix}\bar{C}_1 \bar{D}_1\end{bmatrix}$, in

$$\Sigma^{1D}(A_{22}, \bar{B}_2, C_2, \bar{D}_2).$$

Thus it is clear that the former model realizes the same code as the latter, with the same dimension. So $\Sigma^{1D}(A_{22}, J, C_2, H)$ is a minimal code realization. □

*Example* 5.7. Consider the following composition encoder

$$G(d_1, d_2) = \begin{bmatrix} d_2 + d_1 d_2 & 1 \\ 0 & d_2^2 + d_1 d_2^2 \\ d_2 + d_1 d_2 + d_1 + 1 & 0 \\ 0 & d_2^2 + d_1 d_2^2 + d_1 + 1 \\ 1 & 1 \\ d_2 + d_1 d_2 & d_2^2 + d_1 d_2^2 \end{bmatrix}.$$

It is easy to factorize $G(d_1, d_2)$ as in (5.1) where

$$G_2(d_2) = \begin{bmatrix} d_2 & 1 & d_2 & 0 \\ 0 & d_2^2 & 0 & d_2^2 \\ d_2 + 1 & 0 & d_2 + 1 & 0 \\ 0 & d_2^2 + 1 & 0 & d_2^2 + 1 \\ 1 & 1 & 0 & 0 \\ d_2 & d_2^2 & d_2 & d_2^2 \end{bmatrix} \quad \text{and} \quad G_1(d_1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ d_1 & 0 \\ 0 & d_1 \end{bmatrix},$$

which is canonical and therefore minimal. $G_2(d_2)$ is a quasi-systematic encoder since

$$G_2(d_2) = T \begin{bmatrix} \bar{G}_2(d_2) \\ I_4 \end{bmatrix},$$

with $T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$ invertible and $\bar{G}_2(d_2) = \begin{bmatrix} d_2 & 0 & d_2 & 0 \\ 0 & d_2^2 & 0 & d_2^2 \end{bmatrix}$.

Moreover, $\Sigma^{1D}(A_{22}, \bar{B}_2, C_2, \bar{D}_2)$, where

$$A_{22} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad \bar{B}_2 = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad C_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \text{ and } \bar{D}_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

and $\Sigma^{1D}(A_{11}, B_1, \bar{C}_1, \bar{D}_1)$, where

$$A_{11} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \bar{C}_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \bar{D}_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

are both 1D minimal realizations of $G_2(d_2)$ and $G_1(d_1)$, respectively, and $\begin{bmatrix} \bar{C}_1 & \bar{D}_1 \end{bmatrix} = I_4$ is invertible. Thus, by Theorem 5.6,

$$\Sigma_{2D} = (A_{11}, A_{21}, A_{22}, B_1, B_2, C_1, C_2, D),$$

where

$$A_{11} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \; A_{21} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \; A_{22} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

$$B_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; B_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \; C_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$C_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix} \text{ and } D = \begin{bmatrix} 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$$

is a minimal realization of the 2D convolutional code generated by $G(d_1, d_2)$. ◇

# Chapter 6

# Conclusions

Similarly to what happens for the 1D case, the interconnection between convolutional coding and systems theory is fundamental in order to better understand the issues related with the minimality of 2D convolutional codes.

The ambitious objective of this thesis concerns the characterization of 2D polynomial encoders with minimal McMillan degree and the subsequent construction of minimal 2D code realizations.

Although this has revealed to be a very hard problem, we were able, on the one hand, to generalize some results obtained in [31] and, on the other hand, to apply results from the behavioral approach to 2D convolutional codes achieving some conclusions for particular types of codes.

In Chapter 3 we provided a procedure to obtain a minimal realization of a 1D convolutional code from a minimal realization of an arbitrary encoder of the code.

In Chapters 4 and 5 we have studied the minimality of the realizations of 2D convolutional codes by separable Roesser models. In Chapter 4 we have shown that, similarly to the 1D case, the minimal encoders (i.e., encoders for which a minimal realization is also minimal as a code realization) of a 2D convolutional code of rate $1/n$ are the right factor prime encoders.

In Chapter 5 we introduced a special class of 2D convolutional codes and encoders, namely composition codes and composition encoders. Such codes are characterized by be-

ing generated by encoders that are obtained through the composition of two 1D encoders. Moreover we have analyzed the minimality of realizations for a particular class of composition codes. Concretely we proved that composition encoders are minimal if they can be factorized as a product of a systematic encoder in one indeterminate and a suitable 1D minimal encoder in the other indeterminate.

An interesting problem that we would like to consider in the future is the extension of these results to all composition codes in order to provide a more comprehensive framework on minimality. We believe that the decomposition of 2D convolutional codes into two 1D convolutional codes can increase their impact by allowing to apply known approaches for the 1D case.

Minimal realizations have been widely used in 1D convolutional codes, not only for construction of good codes, but also for the implementation of efficient decoding algorithms. Since the separable Roesser models can be obtained from two 1D realizations, we think that 1D constructions of good convolutional codes can be used to construct good 2D convolutional codes. The construction of optimal 2D convolutional codes of rate $1/n$ was solved in [29] for a very particular case. The general construction of such codes with optimal distance is still an open problem. Similarly, 1D decoding algorithms can be used to implement decoding algorithms for 2D convolutional codes. As far as we know, there is no decoding algorithm available for 2D convolutional codes. This issues constitute a challenging work to be done in the future.

# Appendix A

In this appendix we summarize some basic definitions and results concern the properties of controllability and observability of 1D systems. For more detail we refer to [2, 18].

Let $\Sigma^{1D}(A,B,C,D)$ denote the state-space model

$$\begin{cases} \sigma x(t) = Ax(t) + Bu(t) \\ w(t) = Cx(t) + Du(t), \end{cases} \tag{A.1}$$

where the matrices $A$, $B$, $C$ and $D$ are, respectively, of sizes $m \times m$, $m \times k$, $n \times m$ and $n \times k$.

**Definition A.1.** The pair $(A,B)$ is said to be *controllable if*

$$\operatorname{rank} \left[ B \;\middle|\; AB \;\middle|\; \cdots \;\middle|\; A^{m-1}B \right] = m.$$

**Theorem A.2.** *$(A,B)$ is a controllable pair if and only if*

$$\operatorname{rank} \left[ \lambda I_m - A \;\middle|\; B \right] = m, \quad \forall \lambda \in \bar{\mathbb{F}},$$

*where $\bar{\mathbb{F}}$ denotes the algebraic closure of the field $\mathbb{F}$.*

**Theorem A.3.** *If $(A,B)$ is a controllable pair, for every polynomial $\Pi(\lambda) = \lambda^m + \Pi_{m-1}\lambda^{m-1} + \cdots + \Pi_0$, there exists a matrix $K$ of size $k \times m$ such that the characteristic polynomial of $A - BK$ coincides with $\Pi(\lambda)$, i.e., such that*

$$\det(\lambda I_m - (A - BK)) = \Pi(\lambda).$$

**Corollary A.4.** *(Pole placement) If $(A,B)$ is a controllable pair, for every list $(\lambda_1, m_1), \ldots, (\lambda_r, m_r)$ such that $\lambda_j \in \bar{\mathbb{F}}$, $m_j \in \mathbb{N}$, $j = 1, \ldots, r$ and $m_1 + \cdots + m_r = m$, there exists a matrix $K$ of size*

*$k \times m$ such that $A - BK$ has eigenvalues $\lambda_1, \ldots, \lambda_r$ with multiplicities $m_1, \ldots, m_r$, respectively.*

**Definition A.5.** The pair $(A, C)$ is said to be *observable if*

$$\operatorname{rank} \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{m-1} \end{bmatrix} = m.$$

**Theorem A.6.** *$(A, C)$ is an observable pair if and only if*

$$\operatorname{rank} \begin{bmatrix} \lambda I_m - A \\ C \end{bmatrix} = m, \quad \forall \lambda \in \bar{\mathbb{F}}.$$

**Theorem A.7.** *(Kalman observability decomposition) Assume that the pair $(A, C)$ is not observable, and that* $\operatorname{rank} \begin{bmatrix} C \\ CA \\ \vdots \\ CA^{m-1} \end{bmatrix} = p < m$. *Then, there exists an invertible matrix $S$ such that $\bar{A} = SAS^{-1}$ and $\bar{C} = CS^{-1}$ are of the form:*

$$\bar{A} = \begin{bmatrix} A_{11} & 0 \\ A_{21} & A_{22} \end{bmatrix} \quad \text{and} \quad \bar{C} = \begin{bmatrix} C_1 & 0 \end{bmatrix},$$

*where $A_{11}$ has size $p \times p$, $C_1$ has size $n \times p$, the remaining matrices have compatible sizes, and the pair $(A_{11}, C_1)$ is observable.*

**Remark A.8.** *Defining moreover, $\bar{x} = Sx$, $\bar{A} = SAS^{-1}$, $\bar{B} = SB$, $\bar{C} = CS^{-1}$, equations (A.1) can be written as*

$$\begin{cases} \sigma \bar{x}(t) = \bar{A}\bar{x}(t) + \bar{B}u(t) \\ w(t) = \bar{C}\bar{x}(t) + Du(t), \end{cases}$$

*which, partitioning $\bar{x} = \begin{bmatrix} \bar{x}_1 \\ \bar{x}_2 \end{bmatrix}$ and $\bar{B} = \begin{bmatrix} \bar{B}_1 \\ \bar{B}_2 \end{bmatrix}$ in the obvious way, yields*

$$\begin{cases} \sigma\bar{x}_1(t) = A_{11}\bar{x}_1(t) + \bar{B}_1u(t) \\ \sigma\bar{x}_2(t) = A_{21}\bar{x}_1(t) + \bar{A}_{22}\bar{x}_2(t) + \bar{B}_2u(t) \\ w(t) = \bar{C}_1\bar{x}_1(t) + Du(t). \end{cases}$$

*It is clear from these equations that equation* $\sigma\bar{x}_2(t) = A_{21}\bar{x}_1(t) + \bar{A}_{22}\bar{x}_2(t) + \bar{B}_2u(t)$ *is superfluous, both for the description of the input-output relation between u and w and for the description of the corresponding output behavior (i.e., the behavior of the variable w). This yields an alternative description (of smaller state dimension):*

$$\begin{cases} \sigma\bar{x}_1(t) = A_{11}\bar{x}_1(t) + \bar{B}_1u(t) \\ w(t) = \bar{C}_1\bar{x}_1(t) + Du(t). \end{cases}$$

# References


[1] S. Attasi. Systèmes linéaires homogènes à deux indices. Technical report, Rapport Laboria, 1973. {5,42}

[2] C. Chen. *Linear System Theory and Design*. Oxford University Press, New York Oxford, 1999. {89}

[3] J. J. Climent, D. Napp, C. Perea, and R. Pinto. A construction of MDS 2D convolutional codes of rate $1/n$. *Linear Algebra Appl.*, 437:766–780, 2012. {3}

[4] D. Costello. *Construction of Convolutional Codes for Sequential Decoding*. University of Notre Dame, August, 1969. {20}

[5] P. Elias. Coding for noisy channels. *IRE Conv. Rec.*, Part 4:37–47, 1955. {2}

[6] E. Fornasini. Dispensa di sistemi multivariabili. University of Padua, Italy, 2002. {9,11,12,13,17,19,20}

[7] E. Fornasini and G. Marchesini. Algebraic realization theory of two-dimensional filters. In A. Ruberti and R. Mohler, editors, *Variable Structure Systems with Application to Economics and Biology*, volume 111 of *Lecture Notes in Economics and Mathematical Systems*, pages 64–82. Springer, 1975. {5,42}

[8] E. Fornasini and G. Marchesini. Structure and propertes of two-dimensional systems. In S. G. Tzafestas, editor, *Multidimensional systems : techniques and applications*, volume 29 of *Electrical engineering and electronics*, pages 37–88. Marcel Dekker, 1986. {42}

[9] E. Fornasini and R. Pinto. Matrix fraction descriptions in convolutional coding. *Linear Algebra Appl.*, 392:119–158, 2004. {3,5,27,28,30,59,60,76}

[10] E. Fornasini and M. E. Valcher. Algebraic aspects of two-dimensional convolutional codes. *IEEE Trans. Inform. Theory*, 40(4):1068–1082, 1994. {4,9,22,23}

[11] G. Forney. Convolutional codes I: Algebraic structure. *IEEE Trans. Inform. Theory*, 16(6):720–738, 1970. {2,17,18,59,76}

[12] G. Forney. Minimal bases of rational vector spaces, with applications to multivariable systems. *SIAM J. Control*, pages 493–520, 1975. {2,30,59}

[13] G. Forney. Algebraic structure of convolutional codes, and algebraic system theory. In A. Antoulas, editor, *Mathematical System Theory*, pages 527–557. Springer Berlin Heidelberg, 1991. {2}

[14] F. Gantmacher. *The Theory of Matrices*, volume 1. Chelsea Publishing Company, 1977. {9}

[15] H. Gluesing-Luerssen, J. Rosenthal, and P. A. Weiner. Duality between multidimensional convolutional codes and systems. In F. Colonius, U. Helmke, F. Wirth, and D. Pratzel-Wolters, editors, *Advances in Mathematical Systems Theory, A Volume in Honor of Diedrich Hinrichsen*, pages 135–150. Birkhäuser Boston, 2000. {4}

[16] R. Hamming. Error detecting and error correcting codes. *Bell Syst. Tech.*, 29:147–160, 1950. {2}

[17] T. Hinamoto. Realizations of a state-space model from two-dimensional input-output. *IEEE Trans. Circuits and Systems*, 27:36–44, 1980. {5,46,48,50,53}

[18] T. Kailath. *Linear Systems*. Prentice Hall, Englewood Cliffs, 1980. {9,11,13,27,28,89}

[19] R. E. Kalman. Mathematical description of linear dynamical systems. *SIAM J. Control*, 1(2):152–192, 1963. {2,28}

[20] S. Kung, B. C. Levy, and M. Morf. New results in 2-D systems theory, part I: 2-D polynomial matrices, factorization, and coprimeness. *Proc. IEEE*, 65:861–872, 1977. {15}

[21] S. Kung, B. C. Levy, M. Morf, and T. Kailath. New results in 2-D systems theory, part II: 2-D state-space models — realization and the notions of controllability, observability, and minimality. *Proc. IEEE*, 65:945–961, 1977. {44,45,48}

[22] R. G. Lobo, D. L. Bitzer, and M. A. Vouk. Locally invertible multivariate polynomial matrices. In Ø. Ytrehus, editor, *Coding and Cryptography*, volume 3969 of *Lecture Notes in Computer Science*, pages 427–441. Springer, 2006. {4}

[23] B. Lévy. *2D Polynomial and Rational Matrices, and their Applications for the Modeling of 2-D Dynamical Systems*. Ph.d. dissertation, Stanford University, USA, 1981. {9,22}

[24] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Mathematical Library. Elsevier Science, 1977. {2}

[25] J. L. Massey. Threshold decoding. Technical report, 410, MIT, Research Laboratory of Electronics, 1963. {2}

[26] J. L. Massey and M. K. Sain. Codes, automata, and continuous system: Explicit interconnections. *IEEE Trans. Automat. Control*, 12(6):644–650, 1967. {2,18}

[27] J. L. Massey and M. K. Sain. Inverses of linear sequencial circuits. *IEEE Trans. Comput.*, C-17(4):330–337, 1968. {2,18}

[28] R. J. McEliece. The algebraic theory of convolutional codes. In V. Pless, W. Huffman, and R. A. Brualdi, editors, *Handbook of Coding Theory*, volume 1, pages 1065–1138. Elsevier, Amsterdam, 1998. {2}

[29] D. Napp, C. Perea, and R. Pinto. Input-state-output representations and constructions of finite support 2D convolutional codes. *Adv. Math. Comm.*, 4(4):533–545, 2010. {4,88}

[30] T. Pinho, R. Pinto, and P. Rocha. Realization of 2D convolutional codes of rate $\frac{1}{n}$ by separable roesser models. *Des. Codes Cryptogr.*, 70:241–250, 2014. {4}

[31] R. Pinto. *Matrix Fraction Descriptions in Convolutional Coding*. Ph.d. dissertation, University of Aveiro, Portugal, 2003. {2,17,21,87}

[32] P. Piret. *Convolutional Codes: an Algebraic Approach*. MIT Press, Cambridge, MA, USA, 1988. {2,18}

[33] P. Rocha. *Structure and Representation of 2-D Systems*. Ph.d. dissertation, Rijkuniversiteit Groningen, The Netherlands, 1990. {9,14,15}

[34] P. Rocha. Representation of noncausal 2d systems. In *New Trends in Systems Theory*, volume 7 of *Progress in Systems and Control Theory*, pages 630–635. Birkhäuser Boston, 1991. {49,54}

[35] R. P. Roesser. A discrete state-space model for linear image processing. *IEEE Trans. Automat. Control*, 20(1):1–10, 1975. {5,42,44,45,46}

[36] R. P. Roesser and D. D. Givone. Minimization of multidimensional linear iterative circuits. *IEEE Trans. Comput.*, C-22(7):673–678, 1973. {43}

[37] J. Rosenthal and J. Schumacher. Construction of convolutional codes using methods from linear systems theory. In *Proceedings of the 35-th Annual Allerton Conference on Communication, Control, and Computing*, pages 953–960, 1997. {4}

[38] J. Rosenthal, J. Schumacher, and E. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, 42(6, part 1):1881–1891, 1996. {4}

[39] J. Rosenthal, J. M. Schumacher, and E. V. York. On behavior and convolutional codes. *IEEE Trans. Inform. Theory*, 42(6):1881–1891, 1996. {18}

[40] J. Rosenthal and E. V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, 45(6):1833–1844, 1999. {4}

[41] C. Shannon. A mathematical theory of communication. *Bell Syst. Tech.*, 27:379–423, 623–656, 1948. {1}

[42] R. Smarandache and J. Rosenthal. A state space approach for constructing mds rate $1/n$ convolutional codes. In *1998 Information Theory Workshop*, pages 116–117, 1998. {4}

[43] M. E. Valcher and E. Fornasini. On 2D finite support convolutional codes. *Multidimens. Systems Signal Process.*, 5:231–243, 1994. {4,9,15}

[44] A. J. Viterbi. Error bounds for convolutional codes and an ssymptotically optimum decoding algorithm. *IEEE Trans. Inform. Theory*, 13(2):260–269, 1967. {2}

[45] P. A. Weiner. *Multidimensional Convolutional Codes*. Phd dissertation, Department of Mathematics, University of Notre Dame, Indiana, USA, 1998. {4}

[46] J. C. Willems. Models for dynamics. In U. Kirchgraber and H. O. Walther, editors, *Dynamics Reported*, volume 2, pages 171–269. John Wiley & Sons Ltd., Chichester, 1989. {2,26,31,32}

[47] J. Wozencraft. Sequential decoding for reliable communication. *IRE Nat. Conv. Rec.*, 5(Part 2):11–25, 1957. {2}

[48] D. Youla and G. Gnavi. Notes on n-dimensional system theory. *IEEE Trans. Circuits and Systems*, 26:105–111, 1979. {16}